KEVIN D. MITNICK
SCRITTO CON WILLIAM L. SIMON
L'ARTE DELL'INGANNO
I CONSIGLI DELL'HACKER PIÙ FAMOSO DEL MONDO
Introduzione di Steve Wozniak
Feltrinelli

VISIT…

Kevin Mitnick
(scritto con William L. Simon)
L'arte dell'inganno
I consigli dell'hacker più famoso del mondo

Introduzione di Steve Wozniak
Traduzione di Giancarlo Carlotti
Consulenza scientifica di Raoul Chiesa

Feltrinelli

Titolo dell'opera originale
THE ART OF DECEPTION
O 2002 by Kevin D. Mitnick

Traduzione dall'americano di
GIANCARLO CARLOTTI
Consulenza scientifica di
RAOUL CHIESA

© Giangiacomo Feltrinelli Editore Milano
Prima edizione in "Serie Bianca" ottobre 2003

ISBN 88-07-17086-8

Dedicato a Reba Vartanian, Shelly Jaffe, Chickie Leventhal e Mitchell Mitnick, e alla memoria di Alan Mitnick, Adarn Mitnick e Jack Biello

Per Arynne, Victoria, e David, Sheldon, Vincent ed Elena

Ingegneria sociale

Ingegneria sociale significa l'uso del proprio ascendente e delle capacità di persuasione per ingannare gli altri, convincendoli che l'ingegnere sociale sia quello che non è oppure manovrandoli. Di conseguenza l'ingegnere sociale può usare la gente per strapparle informazioni con o senza l'ausilio di strumenti tecnologici.

Premessa

Noi esseri umani nasciamo con un'intima propensione a esplorare la natura di quanto ci circonda. Da giovani, sia Kevin Mitnick sia il sottoscritto, eravamo curiosissimi del mondo e smaniosi di metterci alla prova. Spesso i nostri tentativi di imparare cose nuove, risolvere enigmi e imporci nel gioco venivano premiati. Ma nel frattempo il mondo attorno a noi ci insegnava anche le regole di comportamento che limitavano le nostre pulsioni all'esplorazione illimitata. Nel caso dei più audaci scienziati e imprenditori del settore tecnologico, e anche di persone come me e Kevin Mitnick, la soddisfazione di questo bisogno interiore garantisce i brividi più intensi mentre facciamo cose che altri ritengono impossibili.

Kevin Mitnick è una delle persone migliori che conosca. Se glielo chiedete lui vi dirà schiettamente che la cosa che praticava, l'ingegneria sociale, significava fregare la gente. Però Kevin non è più un ingegnere sociale. E anche quando lo era non era minimamente intenzionato ad arricchirsi o arrecare danno agli altri. Non sto dicendo che non esistano criminali pericolosi e nocivi che utilizzano l'ingegneria sociale per infliggere danni concreti. Anzi, Kevin ha scritto il presente libro proprio per questo motivo, per mettervi in guardia.

L'arte dell'inganno dimostra quanto siamo vulnerabili, tutti, governo, imprese e ciascuno di noi individualmente, alle intrusioni degli ingegneri sociali. In questa epoca attenta alla sicurezza, investiamo enormi somme in strumenti pensati per proteggere le nostre reti informatiche e i nostri dati. Questo libro illustra quanto sia facile ingannare chi dispone dell'accesso alle informazioni e grazie a lui aggirare tutto questo sbarramento tecnologico.

Che tu lavori in un'impresa o per il governo, questo libro ti regala un efficace manualetto per aiutarti a capire come lavorano

gli ingegneri sociali e cosa puoi fare per contrastarli. In una serie di storielle divertenti quanto illuminanti, Kevin e il coautore Bill Simon inscenano le tecniche del mondo oscuro dell'ingegneria sociale e poi, alla fine di ogni aneddoto, forniscono i consigli pratici per aiutarti contro le intrusioni e le minacce appena descritte.

La sicurezza tecnologica lascia aperti varchi enormi che le persone come Kevin possono aiutare a colmare. Se leggerai questo libro potrai finalmente capire che abbiamo tutti quanti bisogno di rivolgerci per un consiglio ai vari Mitnick che abbiamo vicino.

Steve Wozniak

Prefazione

Alcuni hacker distruggono i file della gente o interi dischi fissi: sono quelli che chiamiamo ***cracker*** o ***vandali.*** Alcuni hacker novellini ***(lamer)*** non sprecano un minuto di tempo a studiare la tecnologia, ma si limitano a scaricare gli strumenti utili per intrufolarsi nei sistemi informatici: sono gli ***script kiddies.*** Quelli più esperti e capaci di programmare sviluppano software che poi postano in Rete o nelle BBS. Infine ci sono i singoli per nulla interessati alle macchine ma che usano i computer soltanto come strumento per rubare soldi, beni, servizi.

Nonostante il mito di Kevin Mitnick creato dalla stampa, io non sono un hacker malintenzionato.

Però non anticipiamo le cose.

Gli inizi

La mia strada dev'essere stata tracciata sin dalla culla. Da bambino ero abbastanza spensierato ma mi annoiavo da morire. Mio padre se ne andò quando avevo tre anni, e mia madre fu costretta a mettersi a lavorare come cameriera per mantenerci. Se mi aveste incontrato in quei giorni, figlio unico di una madre dalle giornate lunghe e impegnate, con orari inaffidabili, avreste visto un giovane lasciato a se stesso in quasi tutte le sue ore da sveglio. Ero la mia baby-sitter.

In compenso avevo la fortuna di abitare in un centro della San Fernando Valley, una cosa che significava la possibilità d'esplorare l'intera Los Angeles. Così già all'età di dodici anni avevo scoperto la maniera di viaggiare gratuitamente in tutta l'area metropolitana. Un giorno, mentre ero in autobus, compresi che la sicurezza del biglietto cumulativo che avevo comprato si basava sulle sempre diverse obliterazioni degli autisti per timbrare

giorno, ora e percorso sui biglietti. In risposta alle mie domande astute, un autista molto gentile mi spiegò dove potevo comprare quei punzonatori.

I biglietti cumulativi permettono di cambiare autobus per proseguire il viaggio fino a destinazione, ma io riuscii a sfruttarli per andare gratis dove mi pareva. Era una passeggiata ottenere gli scontrini in bianco. I cestini nelle stazioni delle autocorriere erano sempre pieni di libretti usati solo in parte, gettati dagli autisti alla fine del turno. Con un tot di biglietti in bianco e il punzonatore potevo obliterare il mio scontrino e recarmi gratis dovunque si spingesse la rete losangelina, In poco tempo memorizzai tutte le linee dell'intero sistema. (E solo un esempio precoce della mia stupefacente memoria per certi tipi d'informazione. Ancora oggi ricordo numeri di telefono, password e altri dettagli apparentemente futili della mia infanzia.)

Un altro interesse affiorato in tenera età è stato quello per la prestidigitazione. Una volta capito come funzionava un trucco, mi esercitavo, esercitavo ed esercitavo fino a quando non ne diventavo maestro. In un certo senso è stata la magia a farmi scoprire le gioie di quando ci si impossessa di saperi segreti.

Da phveak telefonico a hackev

Il mio primo incontro con quella che avrei imparato a chiamare ***ingegneria sociale*** awenne durante il liceo quando conobbi un altro studente che aveva l'hobby del ***phreaking telefonico****, una forma di pirateria che permette di esplorare la rete telefonica sfruttando i sistemi e i dipendenti dell'azienda erogatrice del servizio. L'amico mi mostrò i trucchetti che era capace di combinare con l'apparecchio, tipo come ottenere le informazioni che l'azienda telefonica conserva su ogni cliente e usare un numero segreto di collaudo per fare interurbane gratis. (In realtà erano gratis solo per noi. Molto più tardi ho scoperto che non era affatto un numero segreto. Le chiamate erano addebitate a qualche povero account su MCI.)**

Fu il mio ingresso nell'ingegneria sociale, in un certo senso il mio asilo nido. Il mio amico e un altro phreaker che conobbi poco tempo dopo mi permettevano di starli a sentire quando face-

*** Tecnica di pirataggio telefonico scoperta da Capt. Crunch negli anni sessanta. Successivamente verranno inventati numerosi sistemi (o boxes) (hardware e poi software) per poter telefonare gratuitamente. È una tecnica ancora adesso molto studiata nel mondo dell'hacking, N.d.R.**

**** MCI è una delle maggiori "Telco" (compagnie telefoniche) Usa, insieme ad AT&T, GTF ecc. Un "account" corrisponde a un abbonato al servizio, e alla sua bolletta telefonica, N.d.R.**

vano le chiamate ***pretesto*** all'azienda telefonica, e così ebbi modo di ascoltare le cose che dicevano per risultare credibili, memorizzai le diverse procedure, i gerghi e la struttura delle varie compagnie telefoniche. Comunque questo "apprendistato" non durò molto, non era necessario. Dopo poco tempo facevo già per conto mio, imparando in corsa, con risultati anche più lusinghieri di quelli dei miei primi maestri.

La strada che la mia vita avrebbe seguito nei quindici anni a venire era stata tracciata.

Al liceo uno dei miei scherzi preferiti era accedere non autorizzato al centralino telefonico per cambiare la classe d'utenza di un amico. Quando lui tentava di telefonare da casa sentiva un messaggio che gli diceva di infilare una monetina perché il commutatore centrale aveva ricevuto un segnale indicante che stava chiamando da una cabina.

Mi tuffai a capofitto in tutto quello che riguardava i telefoni, non solo nei circuiti, commutatori e computer, ma anche nell'organizzazione aziendale, nelle procedure e nella terminologia. Dopo un po' mi sa che ero più informato sul sistema telefonico di qualsiasi dipendente. E nel contempo affinai le mie capacità di ingegnere sociale a tal punto che, a diciassette anni, ero in grado di discutere con un professionista del ramo telecomunicazioni su qualsiasi argomento, che fosse a quattr'occhi o per telefono.

La mia tanto strombazzata carriera di hacker è iniziata in realtà quando ero al liceo. Anche se non posso entrare nei dettagli, vi basti sapere che una delle pulsioni che mi spinsero a compiere i primi passi fu il desiderio di essere accettato dal gruppo degli hacker.

A quei tempi si usava la parola ***hacker*** per intendere uno che passava un sacco di tempo a manipolare hardware e software, o per approntare programmi più efficienti, oppure per semplificare certi passaggi inutili in modo da lavorare più in fretta. Adesso è diventata quasi un'offesa, "criminale malintenzionato", ma in queste pagine userò questa parola come l'ho sempre usata, nel senso più benevolo e storico del termine*.

Dopo il liceo passai a studiare informatica al Computer Learning Center di Los Angeles. Nel giro di pochi mesi il direttore dell'istituto si accorse che avevo trovato i punti deboli del sistema operativo ottenendo carta bianca sui loro mini IBM. I migliori informatici del corpo insegnante non riuscivano a capire come c'ero riuscito. In quello che forse fu uno dei primi esempi della politica di assumere gli hacker, mi fecero un'offerta che non potevo rifiutare: o miglioravo il sistema informatico dell'istituto

*** La storia sociale dell'hacking più accreditata è quella riportata nel libro di Steven Levy, *Hackers*, ShaKe, Milano 1994, N.d.R.**

come tesi di diploma oppure sarei stato sospeso per averlo bucato. Naturalmente scelsi la tesi e mi diplomai con lode e bacio accademico.

Diventare ingegnere sociale

Certuni si alzano dal letto alla mattina temendo già la routine della giornata lavorativa. Io sono stato tanto fortunato da amare il mio lavoro. Immaginatevi il piacere, la soddisfazione e il senso di sfida che provavo quando facevo l'investigatore privato. Affinavo il mio talento nell'arte chiamata "ingegneria sociale" (convincere la gente a fare qualcosa che di norma non farebbe per un estraneo) ed ero persino pagato.

Non mi riuscì difficile diventare bravo. Dal lato di mio padre ero nel ramo vendite da generazioni, perciò l'arte della persuasione dev'essere stato un carattere ereditario. Se la combinate con la tendenza al raggiro, otterrete il profilo del perfetto ingegnere sociale.

Potremmo dire che ci sono due specializzazioni nel settore artisti del raggiro. La persona che frega i soldi alla gente appartiene al sottogruppo dei truffatori. Colui che usa l'inganno, il fumo negli occhi e la persuasione contro le imprese, di solito a scapito delle loro informazioni riservate, appartiene all'altro sottogruppo, quello degli ingegneri sociali. Dai giorni dei miei giochetti con i biglietti dell'autobus, quando ero troppo piccolo per capire cosa c'era di male in quel che facevo, ho iniziato a scorgere in me un talento speciale nello scoprire segreti che in teoria non dovevo apprendere. E mi sono basato su questa dote innata aggiungendo l'inganno, imparando il gergo e affinando un discreto bernoccolo per la manipolazione.

Per sviluppare la mia abilità professionale, se posso chiamarla professione, sceglievo per esempio un'informazione che non m'interessava solo per vedere se riuscivo a convincere qualcuno all'altro capo del filo a fornirmela, così, tanto per tenermi in esercizio. Inoltre mi addestravo con i trucchi magici, i pretesti. E grazie a tutto questo allenamento mi ritrovai presto a essere in grado di ottenere tutte le informazioni a cui miravo.

Come ho detto anni dopo, nella deposizione al Congresso davanti ai senatori Lieberman e Thompson:

> Ho ottenuto accesso non autorizzato ai sistemi informatici di alcune delle più grandi aziende del pianeta, e mi sono infiltrato con successo nei sistemi più inaccessibili mai sviluppati. Ho utilizzato metodi tecnologici e non per ottenere il codice sorgente di svariati sistemi operativi e strumenti delle telecomunicazioni, per studiarne la loro vulnerabilità e il funzionamento interno.

Tutte queste attività servivano soltanto a soddisfare la mia curiosità innata, per vedere cosa ero in grado di fare e scoprire informazioni segrete su sistemi operativi, cellulari e tutto quanto mi stimolasse.

Considerazioni finali

Dopo il mio arresto ho ammesso che le mie azioni erano illegali e di avere invaso la privacy altrui. Ma le mie malefatte erano spinte dalla curiosità. Volevo sapere tutto su come funzionavano le reti telefoniche e la sicurezza informatica. Ero un bambino che amava esibirsi nei giochi di magia e adesso sono diventato il più famoso hacker del mondo, temuto da multinazionali e governi. Ora che rifletto sui miei ultimi trent'anni di vita, ammetto di aver preso delle decisioni sbagliate, spinto dalla curiosità, dal desiderio di imparare sempre più cose sulla tecnologia e dalla fame di interessanti sfide intellettuali.

Adesso sono cambiato. Sfrutto il mio talento e il sapere sterminato che ho accumulato sulle tattiche dell'ingegneria sociale per aiutare governo, aziende e singoli a prevenire, individuare e controbattere le minacce portate alla sicurezza dell'informazione.

Questo libro è un modo ulteriore per usare la mia esperienza aiutando gli altri a evitare i tentativi dei malintenzionati ladri di informazioni di tutto il mondo. Credo che troverete divertenti, illuminanti e istruttive le storie che seguono.

Introduzione

Questo libro contiene una notevole mole di notizie sulla sicurezza delle informazioni e l'ingegneria sociale. Per aiutarvi a orientarvi, ecco un primo schizzo di come è organizzato il testo.

Nella prima parte tratterò gli anelli più deboli della sicurezza dimostrandovi perché voi e la vostra azienda siete a rischio di attacchi da parte degli ingegneri sociali.

Nella seconda parte vedrete come questi si facciano beffe della vostra fiducia, del vostro desiderio di dimostrarvi utili, della vostra simpatia e dabbenaggine per ottenere quel che vogliono. Le storielle che illustreranno alcuni attacchi tipici vi dimostreranno come gli ingegneri sociali possano indossare tante uniformi e tante maschere. Se pensate di non averne mai incontrati, probabilmente vi sbagliate. Riconoscerete in questi aneddoti una vicenda che avete già vissuto, e vi interrogherete se per caso avete avuto in quell'occasione un incontro ravvicinato con il social engineering. Possibilissimo. Però quando avrete letto i capitoli dal 2 al 9 saprete come cavarvela quando vi chiamerà il prossimo ingegnere sociale.

La terza parte è quella in cui vedrete come l'ingegnere sociale alza la posta, e lo capirete attraverso alcune storie inventate che dimostreranno come può infiltrarsi nei vostri locali aziendali, rubare i segreti che possono mandare a scatafascio la compagnia ed eludere le misure di sicurezza. I racconti di questa sezione vi faranno capire che i pericoli possono annidarsi dalla vendetta del singolo dipendente al cyberterrorismo. Se ci tenete alle informazioni che fanno andare avanti la vostra azienda e alla privacy dei dati, vi consiglio di leggere i capitoli dal 10 al 14, dall'inizio alla fine. È importante ricordare che gli aneddoti presentati nel libro, a meno che non venga segnalato altrimenti, sono totalmente inventati.

Nella quarta parte discuterò con linguaggio più "aziendale"

come si fa a sventare gli attacchi degli ingegneri sociali alla vostra organizzazione. Il capitolo 15 fornisce lo schema di un utile programma di addestramento alla sicurezza, e il *Vademecum* potrebbe salvarvi la pelle: contiene una completa politica di sicurezza che potrete adattare alla vostra organizzazione e anche arricchire per mettere al sicuro l'azienda e le informazioni.

Alla fine ho redatto una sezione "sicurezza in breve" contenente checklist, tabelle e grafici per riassumere le informazioni cruciali che potrete usare per aiutare i vostri dipendenti a sventare un attacco di ingegneria sociale. Questi strumenti vi daranno anche informazioni preziose per impostare un vostro programma di formazione alla sicurezza.

Inoltre, nel corso di tutto il volume troverete parecchi elementi utili quali i "messaggi di **Mitnick**" (evidenziati in box grafici) che distribuiranno ogni tanto brevi perle di saggezza per aiutarvi a consolidare le strategie di sicurezza.

Prima **parte**

Dietro le quinte

1.
L'anello più debole della sicurezza

Un'azienda potrebbe anche essersi dotata delle migliori tecnologie di sorveglianza, avere addestrato i dipendenti a mettere sotto chiave tutti i segreti prima di smontare la sera e assunto guardie giurate della migliore agenzia del settore.

Ed essere ancora vulnerabile.

I singoli individui possono seguire le migliori tattiche consigliate dagli esperti, installare supinamente tutti i prodotti raccomandati, essere assolutamente rigorosi sull'adatta configurazione di sistema e tempestivi nell'apportare le correzioni del caso.

Ma queste persone sarebbero ancora totalmente vulnerabili.

IL FATTORE UMANO

Quando non molto tempo fa ho deposto davanti al Congresso, ho spiegato che spesso riuscivo a ottenere password e altre informazioni delicate dalle aziende fingendo di essere qualcun altro e *banalmente chiedendole.*

Il naturale desiderio di protezione assoluta spinge molte persone a cullarsi in un falso senso di sicurezza. Pensate al coscienzioso e amorevole proprietario di casa che ha appena installato un "Medico", una serratura comunemente ritenuta a prova di scasso, per proteggere moglie, figli e villetta. Adesso è tutto contento perché si ritiene al riparo dagli intrusi. Ma se questi sfondano una finestra o rubano il codice del basculante del garage? Che ne dite di installare un sistema di sicurezza come si deve? Adesso va meglio, ma non è ancora una garanzia. La vostra casa resterà vulnerabile nonostante tutte le serrature costose.

Perché? Perché il fattore *umano* è sul serio l'anello più debole della sicurezza.

Troppo spesso la sicurezza è solo un'illusione, certe volte aggravata allorché si aggiungono dabbenaggine, ingenuità o ignoranza. Il più prestigioso scienziato del Ventesimo secolo, Albert Einstein, disse un giorno: "Soltanto due cose sono infinite, l'universo e la stupidità umana, e non sono tanto sicuro della prima". Andando all'osso, gli attacchi degli ingegneri sociali possono avere successo se le persone sono stupide o, più spesso, ignare delle buone pratiche di sicurezza. Comportandosi come il nostro coscienzioso proprietario di villetta, molti professionisti della Information Technology (IT) si crogiolano nella presunzione errata di aver reso la loro ditta immune agli attacchi perché hanno usato prodotti standard, firewall, sistemi di rilevamento intrusioni o più forti strumenti di autentica come le smart card biometriche. Chiunque pensi che i prodotti da soli offrano la vera sicurezza si sta cullando soltanto nella sua ***illusione.*** Sta vivendo nel mondo dei sogni. Prima o poi gli capiterà un grosso incidente.

Come ha detto il noto consulente del settore Bruce Schneier: "La sicurezza non è un prodotto, è un processo". Inoltre non è un problema di tecnologia, bensì di persone e gestione.

Man mano che si inventano tecnologie di sicurezza sempre più raffinate, che rendono improbo sfruttare i punti deboli tecnici, gli attaccanti decideranno sempre più spesso di sfruttare l'elemento umano. Spesso sfondare questo tipo di firewall è facile, non richiede alcun investimento oltre il costo di una telefonata, e comporta rischi minimi.

UN CLASSICO CASO DI ATTACCO

Qual è la più grave minaccia alla sicurezza dei vostri beni aziendali? E facile: l'ingegnere sociale, quel mago poco scrupoloso che vi induce a tenere d'occhio la sinistra mentre con la destra vi sgraffigna i segreti. Spesse volte si tratta di un personaggio cordiale, loquace e servizievole che siete contenti di avere incontrato.

Ecco un classico esempio di ingegneria sociale. Oggi pochi ricordano il giovane Stanley Mark Rifkin e la sua awenturetta con l'ormai defunta Security Pacific National Bank di Los Angeles. Le versioni della sua bravata variano, e Rifkin (come me) non ha mai raccontato la sua, perciò quel che segue si basa sui resoconti pubblicati.

Decifrare il codice

Un giorno del 1978, Rifkin gironzolava nella sala telex ad accesso limitato della Security Pacific, dove transitavano trasferimenti monetari di parecchi miliardi di dollari al giorno.

Lavorava per una ditta che doveva approntare un sistema di back-up dei dati della sala nel caso in cui il computer centrale fosse saltato, perciò era informatissimo sulle procedure di trasferimento, compreso come facevano i funzionari a inviare i soldi: i cassieri autorizzati ai bonifici ricevevano tutte le mattine un codice giornaliero strettamente controllato per quando chiamavano la sala telex.

Gli impiegati di quell'ufficio, per evitare di memorizzare ogni giorno il nuovo codice, lo riportavano su un foglietto che appiccicavano in un punto visibile. Quel giorno di novembre Rifkin era venuto per un motivo specifico. Voleva dare un'occhiata proprio a quel foglietto.

Arrivato nella sala prese nota delle procedure, in teoria perché il suo sistema di back-up si ingranasse a puntino con quello normale, e nel frattempo ne approfittò per sbirciare il codice di sicurezza scritto sui foglietti e memorizzarlo. Uscì qualche minuto dopo. Come avrebbe spiegato in seguito, gli sembrava di avere appena vinto alla lotteria.

Ci sarebbe questo conto corrente svizzero...

Quando uscì alle tre del pomeriggio puntò dritto verso la cabina del telefono nell'atrio marmoreo dell'edificio, dove infilò la monetina e fece il numero della sala, poi si riciclò da Stanley Rifkin, consulente bancario, a Mike Hansen, dipendente dell'ufficio estero della banca.

Secondo una fonte affidabile, la conversazione andò più o meno così.

"Ciao, sono Mike Hansen dell'ufficio estero," disse alla giovane che rispose.

Lei gli domandò il suo numero di interno. Essendo informato della procedura standard, Stanley rispose subito: "286".

"Bene, e il codice?"

Rifkin ha raccontato in seguito che a quel punto la sua frequenza cardiaca già in picco di adrenalina "accelerò". Comunque rispose imperturbabile: “4789”, poi diede istruzioni per trasferire “10.200.000 dollari esatti" tramite la Irving Trust Company di New York alla Wozchod Handels Bank di Zurigo dove aveva già aperto un conto.

Allora la giovane disse che andava bene, e che le serviva solo il numero di transazione tra un ufficio e l'altro.

Rifkin iniziò a sudare. Non aveva previsto quella domanda durante le sue ricerche, ma riuscì a non farsi travolgere dal panico, si comportò come se fosse tutto normale e rispose al volo: "Aspetta che controllo e ti richiamo subito". Dopodiché cambiò di nuovo personaggio per telefonare a un altro ufficio della banca, stavolta sostenendo di essere un impiegato della sala telex, ottenne il numero e richiamò la ragazza.

La quale lo ringraziò. (Date le circostanze si tratta di un ringraziamento assai ironico.)

La conclusione

Qualche giorno dopo Rifkin volò in Svizzera, prelevò i soldi e consegnò 8 milioni a un'agenzia russa in cambio di un sacchetto di diamanti, poi tornò in patria, passando attraverso la dogana con le pietre nascoste nella cintura portamonete. Aveva fatto la più grossa rapina in banca della storia, e senza pistole, addirittura senza computer. Stranamente, la sua impresa è finita sul *Guinness dei primati* sotto la categoria 'le più grandi truffe informatiche".

Aveva sfruttato l'arte del raggiro, i talenti e le tecniche che oggi chiamiamo "ingegneria sociale". Gli erano bastate una pianificazione scrupolosa e un po' di parlantina.

Questo libro non parla d'altro: le tecniche dell'ingegneria sociale (in cui il sottoscritto è abbastanza versato) e come difendersi contro il loro utilizzo ai danni della vostra azienda.

LA NATURA DELLA MINACCIA

La storia di Rifkin fa capire perfettamente come possa essere malriposto il nostro senso di sicurezza. Incidenti come questi (d'accordo, forse non rapine da dieci milioni di dollari ma comunque sgradevoli) succedono *tutti i giorni*. Forse state perdendo soldi anche in questo momento oppure qualcuno vi sta rubando i progetti dei nuovi prodotti, senza che nemmeno lo sappiate. Se non è già successo alla vostra ditta non è questione di *se* ma di *quando*.

Una preoccupazione crescente

Il Computer Security Institute, nella sua analisi del 2001 sui crimini informatici, ha segnalato che l'85% delle organizzazioni

che avevano risposto al sondaggio aveva riscontrato falle nella sicurezza nei dodici mesi precedenti. È una cifra impressionante: soltanto il 15% delle organizzazioni ha risposto di non avere subito intrusioni durante l'anno. Altrettanto incredibile era il numero di strutture che segnalavano perdite economiche a causa di intrusioni informatiche: 64%. Ben oltre la metà delle organizzazioni aveva sofferto nel portafoglio. *In* un solo anno.

La mia esperienza mi induce a credere che di regola le cifre che emergono in sondaggi del genere sono inflazionate. Sono sempre sospettoso delle motivazioni di chi conduce la ricerca. Non sto però sostenendo che i danni non siano immani. Lo sono. Chi non programma la sicurezza programma il fallimento.

I prodotti commerciali per la sicurezza usati da quasi tutte le aziende puntano soprattutto a fornire protezione contro l'intruso informatico dilettante, tipo i ragazzini noti come "script kiddies". In realtà questi hacker in erba e i software che scaricano sono solo una rottura, di solito. Le perdite maggiori, le minacce serie, provengono dai nemici sofisticati che hanno in mente uno scopo ben preciso, da gente motivata dai soldi. Costoro prendono di mira un bersaglio per volta invece di fare come i dilettanti che infiltrano più sistemi possibile. Questi cercano la quantità, i professionisti sono alla ricerca di informazioni preziose e di qualità.

Le tecnologie come gli strumenti di autenticazione (per dimostrare l'identità), il controllo dell'accesso (per regolare l'accesso ai file e alle risorse di sistema) e i sistemi di rilevamento delle intrusioni (l'equivalente elettronico dell'allarme antifurto) sono assolutamente necessarie per un programma aziendale di sicurezza. Eppure ancor oggi è normale che un'impresa spenda più soldi per il caffè che per le contromisure per proteggersi dagli attacchi ai vostri dati.

Come la mente del criminale non sa resistere alla tentazione, la mente dell'hacker è spinta a trovare una maniera per aggirare le potenti salvaguardie della tecnologia. E in molti casi ci riesce proprio concentrandosi sulle persone che usano la tecnologia.

Pratiche ingannevoli

Secondo un detto famoso, il solo computer sicuro è quello spento. Arguto, ma inesatto: un pretesto ti convincerà ad andare in ufficio per accenderlo. Un avversario che vuole le tue informazioni riesce sempre a ottenerle, di solito in tanti modi. È solo questione di tempo, pazienza, carisma e insistenza. E qui che entra in gioco l'arte dell'inganno.

Per battere le misure di sicurezza l'assalitore, intruso o ingegnere sociale che sia deve trovare la maniera di ingannare un

utente fidato affinché gli dia informazioni, oppure un bersaglio ignaro perché gli garantisca l'accesso. Quando un dipendente fidato viene ingannato, suggestionato o manipolato in modo da rivelare informazioni cruciali, o compiere azioni che creino una falla nella sicurezza per far passare l'assalitore, nessuna tecnologia al mondo potrà proteggere l'impresa. Come i crittanalisti sono in grado di rivelare il testo in chiaro di un messaggio cifrato grazie al punto debole che consente loro di scavalcare la tecnologia crittografica, alla stessa stregua gli ingegneri sociali usano il raggiro ai danni dei vostri dipendenti per sormontare le tecnologie di protezione.

ABUSO DI FIDUCIA

Nella maggior parte dei casi gli ingegneri sociali sono abilissimi nei rapporti umani, risultano affascinanti, educati e simpatici, tutte doti necessarie per chi desideri stabilire al più presto un rapporto di fiducia. Un esperto ingegnere sociale può accedere praticamente a qualsiasi informazione sfruttando le tattiche e strategie della sua arte.

I tecnocrati più avvertiti hanno sviluppato con assiduità soluzioni di sicurezza atte a minimizzare i rischi connessi all'uso dei computer, ma hanno lasciato irrisolto il punto debole più significativo, il fattore umano. Nonostante il nostro raziocinio, noi umani, voi, io e tutti gli altri, restiamo la più grave minaccia alla sicurezza degli altri.

La nostra caratteristica nazionale

Noi, soprattutto nel mondo occidentale, non mettiamo in conto le aggressioni. Non siamo addestrati a sospettare dell'altro, soprattutto negli Stati Uniti, dove ci insegnano ad "amare il prossimo tuo" e avere fiducia e fede negli altri. Pensate solo a quant'è difficile per le ronde volontarie di vigilanza convincere la gente a chiudere a chiave la casa e l'auto. È una debolezza risaputa, eppure sembra essere ignorata dai tanti che preferiscono vivere in un mondo di sogno... fino a quando non rimangono scottati.

Sappiamo perfettamente che non tutti sono gentili e onesti, ma troppo spesso ci comportiamo come se lo fossero. Questa simpatica innocenza è stata il fulcro della vita degli americani, ed è doloroso lasciarsela alle spalle perché come nazione abbiamo inserito nel nostro concetto di libertà l'idea che il miglior

posto in cui vivere è quello dove non sono necessarie chiavi e serrature.

Quasi tutti si basano sull'assunto che nessuno li ingannerà mai, e ritengono che la probabilità di essere raggirati sia infima. La persona che porta l'attacco, conscia di questa credenza comune, riesce a far sembrare tanto ragionevole la sua richiesta da non sollevare sospetti mentre sfrutta la fiducia della vittima.

Innocenza organizzativa

Questa innocenza come parte del carattere nazionale era al suo apogeo quando collegarono per la prima volta computer lontani. Non è da dimenticare che ARPANet (la rete dell'Agenzia per i progetti avanzati di ricerca del ministero della Difesa), antesignana di Internet, fu progettata per condividere i dati tra le varie strutture governative, di ricerca e universitarie al fine di ottenere una maggiore libertà d'informazione unitamente a un avanzamento tecnologico. Quindi molte strutture universitarie impiantarono i primi sistemi informatici con una sicurezza risibile. Un noto libertario del software, Richard Stallman,* si rifiutò persino di proteggere il suo account con una password.

Ma quando hanno cominciato a usare Internet per il commercio elettronico, gli inconvenienti di una protezione debole nel nostro mondo cablato hanno assunto una dimensione drammatica. Una quantità maggiore di tecnologia non risolverà il problema umano della sicurezza.

Pensiamo solo agli aeroporti di oggi. La sicurezza è diventata onnipresente, eppure rimaniamo sconcertati dai servizi sui viaggiatori che sono riusciti a superare i controlli con armi potenziali. Com'è possibile in un'epoca in cui gli aeroporti sono in stato d'allerta? I metal detector non funzionano? No, il problema non sono le macchine. Il problema è il fattore umano, la gente che usa le macchine. I responsabili aeroportuali possono anche chiamare la Guardia nazionale e installare metal detector e sistemi di riconoscimento del volto, ma sarebbe più utile istruire il personale in prima linea a esaminare come si deve i passeggeri.

Il medesimo problema si presenta nelle strutture statali, imprenditoriali e accademiche di tutto il mondo. Nonostante gli

* Richard Staliman è il presidente della Free Software Association, un'organizzazione composta soprattutto di volontari che ha il fine di costruire un sistema operativo – e i conseguenti applicativi – in grado di soppiantare l'egemonia del cosiddetto "software chiuso". La caratteristica dei loro programmi è di essere rilasciati compresi di codice sorgente. ***[N.d.R.]***

sforzi dei professionisti della sicurezza, l'informazione resta vulnerabile ovunque e continuerà a essere vista come un bersaglio ghiotto da parte dei malfattori pratici di ingegneria sociale fino a quando non sarà rafforzato l'anello debole della catena, quello umano.

Ora più che mai dobbiamo dimenticare i pii desideri ed essere più consapevoli delle tecniche usate da chi tenta di aggredire il riserbo, la disponibilità e l'integrità dei nostri sistemi informatici e relative reti. Abbiamo accettato una guida sicura, adesso è ora di accettare e imparare l'informatica sicura.

La minaccia delle intrusioni nella privacy, nella vostra mente o nei sistemi di informazione di un'impresa può sembrare irreale fino a quando non si concretizza. Per evitare una lezione così costosa di vita vissuta, dobbiamo diventare tutti consapevoli, educati, vigili e aggressivi nella protezione delle nostre informazioni, quelle personali e quelle delle infrastrutture critiche della nazione. E dobbiamo prendere queste precauzioni adesso.

TERRORISTI E RAGGIRO

Certo, il raggiro non è l'esclusiva dell'ingegnere sociale. Il terrorismo riempie le prime pagine dei giornali, e abbiamo capito come mai prima d'ora che il mondo è un posto pericoloso. In fin dei conti la civiltà è solo una patina sottile.

Gli attacchi a New York e Washington del settembre 2001 hanno sconvolto non solo noi americani ma tutte le persone di buona volontà di tutte le nazioni. Abbiamo capito che ci sono terroristi invasati sparsi nel globo, ben addestrati e pronti a lanciare altri attacchi.

Le recenti iniziative del nostro governo hanno aumentato il livello di consapevolezza della sicurezza. Dobbiamo essere vigili, stare in guardia contro ogni forma di terrorismo. Dobbiamo capire come fanno i terroristi a crearsi una falsa identità, come riescono a farsi passare per studenti o vicini e si mischiano nella massa, mascherando la loro vera fede mentre tramano contro di noi, usando trucchi simili a quelli che leggerete su queste pagine.

Anche se, per quanto ne so, costoro non hanno ancora sfruttato l'ingegneria sociale per infiltrarsi in grandi aziende, impianti idrici, centrali elettriche o altre componenti vitali del paese, esiste pur sempre una possibilità. È troppo facile. La presa di coscienza e le politiche relative alla sicurezza che i dirigenti aziendali inaugureranno grazie a questo libro, almeno spero, non arriveranno mai troppo tardi.

QUESTO LIBRO

La sicurezza aziendale è questione di equilibrio. Una scarsa sicurezza lascia vulnerabile l'impresa, ma un eccesso intralcia gli affari, bloccando la crescita e la prosperità dell'azienda stessa. Il problema è come ottenere un bilanciamento tra sicurezza e produttività.

Altri libri sulla sicurezza aziendale parlano soprattutto di hardware e software, ma non coprono in maniera adeguata la minaccia più seria: il raggiro umano. Questo libro, al contrario, vuole aiutarvi a capire come voi, i vostri colleghi e altri nell'organizzazione rischiate di essere manipolati e a immaginare quali barriere potreste erigere per non diventare vittime. Il mio libro parla soprattutto dei metodi non tecnologici usati dagli intrusi ostili per rubare informazioni, compromettere l'integrità di dati ritenuti sicuri ma che non lo sono, oppure scompaginare la produzione aziendale.

È un compito reso più difficile da un banale truismo: ogni lettore è stato manipolato dai massimi esperti di tutti i tempi in tema di ingegneria sociale, i suoi genitori. Loro sanno come indurti a fare ("per il tuo bene") quel che ritengono meglio. I genitori diventano grandi cantastorie proprio come gli ingegneri sociali inventano con abilità plausibilissime scuse, ragioni e giustificazioni per arrivare al loro scopo. ***Sì,*** siamo stati tutti modellati dai nostri genitori, ingegneri sociali in buona fede (non sempre).

Condizionati da questa preparazione, siamo diventati vulnerabili alle manipolazioni. Sarebbe una vita ben amara se stessimo sempre sul chi va là, sospettosi degli altri, preoccupati di non diventare lo zimbello di uno che cerca di sfruttarci. In un mondo perfetto ci fideremmo automaticamente degli altri, saremmo sicuri che la gente che incontriamo è tutta onesta e affidabile. Purtroppo non viviamo in un mondo perfetto, e così dobbiamo applicare uno standard di vigilanza per respingere i raggiri dei nostri nemici.

Le sezioni principali di questo libro, la 2 e la **3,** contengono delle storie che vi dimostreranno come agiscono gli ingegneri sociali. Vi leggerete:

- Quello che hanno scoperto anni fa i phone phreaks: un metodo ingegnoso per ottenere dalla compagnia telefonica un numero che non figura sull'elenco.
- Parecchi metodi diversi usati dagli attaccanti per convincere anche i dipendenti più vigili e sospettosi a svelare username e password.
- Come il responsabile di un centro operativo abbia permesso

a un attaccante di rubare le informazioni sul prodotto più segreto della sua azienda.

- I metodi di un attaccante che ha convinto una signora a scaricare un software che spia ogni tasto da lei premuto e gli invia per posta elettronica tutti i particolari.
- Come fanno gli investigatori privati a ottenere informazioni sulla vostra azienda e su di voi nello specifico, roba che vi garantisco vi farà venire la pelle d'oca.

Mentre leggerete queste storie penserete che sono impossibili, che nessuno può riuscire a farla franca con le bugie e i trucchetti descritti in queste pagine. Purtroppo in tutti i casi gli aneddoti si riferiscono a fatti che sono accaduti e possono succedere, molti dei quali awengono ogni giorno in un punto del pianeta, forse persino nella vostra azienda mentre state leggendo questo libro.

Il materiale contenuto in queste pagine dovrebbe essere illuminante per quanto riguarda la protezione dei vostri affari, ma anche restando sul piano personale dovrebbe riuscire a proteggere l'integrità dei dati sulla vostra vita privata.

Nella quarta parte cambierò marcia. Con quest'ultima sezione vorrei aiutarvi a creare le necessarie politiche e attenzioni aziendali, insegnandovi a minimizzare le probabilità che i vostri dipendenti siano ingannati da un ingegnere sociale. Comprendere le strategie, metodi e tattiche del nemico vi aiuterà a impiantare oculati controlli per proteggere la vostra IT senza compromettere la produttività.

Per farla breve, ho scritto questo libro per rendervi consapevoli della grave minaccia portata dall'ingegneria sociale e per aiutarvi a impedire che la vostra azienda e i suoi dipendenti possano essere sfruttati in questo modo.

O forse farei meglio a dire: a impedire che possano essere sfruttati di ***nuovo.***

Seconda parte

L'arte dell'attaccante

2.
Quando un'informazione innocua non lo è

Qual è la vera minaccia portata dagli ingegneri sociali per la maggior parte della gente? Che cosa dovreste fare per stare in campana?

Se il loro fine è quello di catturare una preda preziosa, che so, una componente essenziale del capitale intellettuale dell'azienda, allora forse vi basteranno, in senso figurato, un caveau più forte e guardie meglio armate. O no?

In realtà la penetrazione della sicurezza di un'azienda inizia spesso con il cattivo che ottiene un'informazione o qualche documento in apparenza innocente, robetta tanto banale e così poco importante che quasi nessuno nella struttura capisce perché dovrebbe essere protetta e riservata.

IL VALORE NASCOSTO DELL'INFORMAZIONE

Quasi tutte le informazioni apparentemente innocue in possesso di un'impresa sono apprezzate dall'ingegnere sociale perché possono giocare una parte essenziale nel suo tentativo di rivestirsi di una patina di credibilità.

In queste pagine vi dimostrerò come agiscono gli ingegneri sociali lasciandovi "assistere" di persona agli attacchi, talvolta presentandovi l'azione dal punto di vista delle vittime, permettendovi così di mettervi nei loro panni e valutare come voi (o forse uno dei vostri dipendenti e colleghi) avreste reagito. In tanti casi vivrete la medesima esperienza anche dal punto di vista dell'ingegnere sociale.

La prima storia ci racconta la vulnerabilità del settore finanziario.

I britannici hanno avuto per secoli un sistema bancario antiquato. Anche se eravate cittadini normali e onesti non potevate andare ad aprire un conto corrente, no, la banca non ci pensava proprio ad accettarvi come correntisti, a meno che un altro cliente noto non vi avesse scritto una lettera di presentazione.

Che differenza con l'odierno sistema bancario apparentemente egualitario! E la disinvoltura moderna nella conduzione degli affari è soprattutto evidente nell'amichevole America democratica, dove quasi tutti possono entrare in banca e aprire un conto come se niente fosse, no? Be', non è esatto. La verità è che le banche, comprensibilmente, sono riluttanti ad aprire un conto a una persona con un passato di assegni **a** vuoto, gradito quanto una fedina penale costellata di rapine in banca o malversazioni. Perciò è pratica corrente in tanti istituti decidere in fretta sul potenziale cliente.

Una delle principali agenzie che forniscono informazioni alle banche è una struttura che chiamaremo CreditChex, la quale fornisce un servizio importante e però, come tante imprese, rende senza saperlo anche un comodo servizio a un ingegnere sociale che sa il fatto suo.

La prima telefonata: Kim Andrews

"National Bank, sono Kim. Desidera aprire un conto?"

"Buongiorno, Kim, avrei una domanda da farle. Usate la CreditChex lì da voi?"

"Sì."

"Quando telefonate alla CreditChex, come chiamate il numero che gli date? E una 'Merchant ID'?"

Pausa. Kirn sta valutando la domanda e si chiede che cosa significa e cosa deve rispondere.

La persona al telefono continua senza perdere un colpo. "Vede, Kim, starei scrivendo un libro sulle investigazioni private."

Allora lei risponde di sì con maggiore convinzione, lieta di poter dare una mano a uno scrittore.

"Allora si chiama Merchant ID?"

"Ah-ah."

"Fantastico. Perché, sa, volevo essere sicuro del gergo. Per il libro, intendo. Grazie del suo aiuto. Arrivederci, Kirn."

La seconda telefonata: Chris Talbert

"National Bank. Nuovi conti correnti, sono Chris."

"Ciao, Chris, sono Alex. Sono responsabile dei servizi alla clientela della CreditChex e stiamo cercando di migliorare le prestazioni. Puoi dedicarmi un paio di minuti?" domanda il chiamante.

Chris sembra disponibile, perciò l'interlocutore inizia: "Allora, che orari fate?". Dopodiché Chris risponde a una serie di domande.

"Quanti dipendenti della vostra filiale usano la nostra struttura?"

"Quanto spesso ci chiamate per un controllo?"

"Quale numero verde vi abbiamo assegnato per chiamarci?"

"I nostri sono sempre stati gentili?"

"Quanto ci mettiamo a rispondere?"

"Da quanto tempo lavori per la banca?"

"Che Merchant ID usi in questo momento?"

"Hai mai riscontrato inesattezze nelle informazioni che vi abbiamo dato?"

"Hai qualche suggerimento per migliorare il servizio?"

E: "Saresti disponibile a compilare i questionari periodici che ti invieremo in sede?"

Lei accetta, poi scambiano due chiacchiere, lui appende e Chris torna al lavoro.

Terza telefonata: Henry McKinsey

"CreditChex, sono Henry McKinsey. In cosa posso esserle utile?"

Il telefonante sostiene di essere della National Bank, dà la Merchant ID e poi il nome e il numero di previdenza della persona su cui desidera informazioni. Quando Henry chiede la data di nascita, l'altro dà anche quella.

Dopo qualche istante Henry legge l'esito sul suo monitor.

"La Wells Fargo ha segnalato un assegno scoperto di 2066 dollari nel 1998."

"Altri movimenti successivi?"

"No."

"Altre richieste di apertura conto?"

"Vediamo. Sì, due, entrambe il mese scorso. Third United Credit Union di Chicago." S'inceppa sul nome seguente, Schenectady Mutual Investment, e gli tocca compitarlo. "E nello stato di New York," aggiunge.

L'investigatore privato *all'opera*

Le tre chiamate sono state fatte dalla stessa persona, un investigatore privato che chiamaremo Oscar Grace, il quale ha un nuovo cliente, uno dei primi. Fino a pochi mesi prima Oscar faceva il poliziotto, e il nuovo lavoro gli riesce facile a parte qualche sfida speciale per la sua inventiva e le sue risorse. Quest'ultimo incarico appartiene decisamente alla categoria delle sfide.

Il detective dei gialli, alla Sam Spade o alla Philip Marlowe, passa lunghe ore notturne seduto in macchina a cercare di cogliere in castagna un coniuge infedele. I veri detective non sono molto diversi, però svolgono un genere meno decantato ma non meno importante di spionaggio, che si basa più sull'ingegneria sociale che su come combattere la noia delle veglie notturne.

Il nuovo cliente di Grace è una signora che ha l'aria di avere parecchi soldi da investire in gioielli e vestiti. È entrata un giorno nel suo ufficio sedendosi sulla poltrona di pelle, l'unica sgombra dai giornali, ha posato la voluminosa borsetta Gucci sulla scrivania con il simbolo girato verso di lui e ha annunciato che stava progettando di comunicare al marito che vuole il divorzio, ammettendo però "qualche problemino".

Pare che il coniuge sia partito in anticipo. Ha appena svuotato i conti e anche una somma più sostanziosa in un fondo di investimento. Ora la cliente vuole sapere dove sono finiti i soldi ma l'avvocato divorzista non può aiutarla. Grace immagina che sia uno di quei legali da grattacielo in centro che non si sporcherebbero mai le mani a cercare del denaro trafugato.

Può aiutarla?

Lui le garantisce che è una sciocchezza, spara una cifra più le spese e ritira l'assegno dell'anticipo.

Poi affronta il problema. Come ti comporti se non hai mai provato una cosa del genere e non sai come seguire la pista dei soldi? Procedi a passettini. Ecco la storia di Grace secondo la nostra fonte.

Sapevo della CreditChex e di come la usano gli istituti bancari. La mia ex moglie lavorava in banca. Però non conoscevo il gergo e le procedure, e chiedere alla mia ex sarebbe stata solo una perdita di tempo.

Primo passo: conoscere la terminologia e capire come porre richieste in modo da avere l'aria di sapere quel che sto facendo. Nella banca a cui ho telefonato la prima signorina, Kim, è parsa un po' sospettosa quando le ho chiesto come si identificano quando telefonano alla CreditChex. Ha esitato, non sapeva come reagire. Mi ha scoraggiato, forse? Nemmeno un po'. Anzi, quell'esitazione mi ha dato un suggerimento importante, il se-

gnale che dovevo fornire un motivo credibile. Quando le ho rifilato la storia delle ricerche per un libro mi è subito parsa meno sospettosa. Se dici che sei uno scrittore o uno sceneggiatore ti si spalancano davanti tutte le porte.

Kim sapeva altre cose utili, come le informazioni che richiede la CreditChex per identificare la persona per cui chiami, quali dati puoi chiedere e quella grossa, il suo codice bancario Merchant ID. Ero lì lì per porre quelle domande, ma la sua esitazione mi aveva messo la pulce nell'orecchio. Ha bevuto la storia del libro, ma aveva già qualche sospetto. Se fosse stata subito più disponibile le avrei chiesto altri dettagli.

Nel mio lavoro devi agire d'istinto, ascoltare attentamente cosa sta dicendo il bersaglio e come lo dice. Questa signorina mi sembrava abbastanza sveglia da far scattare il segnale d'allarme se le chiedevo troppe cose insolite. E anche se lei non sapeva chi fossi o da quale numero chiamavo, in questo tipo di lavoro non vuoi mai che giri la voce che c'è un tale in cerca di informazioni specifiche del settore. È per questo che non vuoi bruciarti la fonte: vuoi essere in grado di richiamare lo stesso ufficio un'altra volta.

Sto sempre attento ai piccoli segnali che mi fanno capire se una persona sta collaborando lungo una scala che va dal "mi sembri un tipo a posto e credo a tutto quello che dici" al "chiamate la polizia, allertate la Guardia nazionale, questo qua mi puzza".

Sentivo che Kim era un tantino tesa, così ho chiamato un'altra filiale. Alla seconda telefonata, quella con Chris, il trucco del controllo ha funzionato che era una bellezza. Sta tutto nel porre una domanda importante in una sfilza che serve a creare un'aura di credibilità. Prima di lasciar cadere la domanda del numero Merchant ID con la CreditChex ho fatto la prova finestra chiedendole un dato personale, cioè da quanto tempo lavorava lì.

La domanda personale è una mina antiuomo, alcuni ci passano sopra senza manco accorgersene, invece con altri scoppia. Perciò se la pongo e lei mi risponde senza che il tono di voce cambi, significa che non è scettica e che posso porre tranquillamente la domanda cruciale senza insospettirla, e probabilmente mi darà la risposta che cerco.

C'è un altro assioma di ogni bravo detective privato: mai interrompere la conversazione una volta ottenuto il dettaglio chiave. Altre due o tre domandine, quattro chiacchiere e poi puoi dire ciao. Così, se la vittima ricorda qualcosa, saranno probabilmente le ultime due domande. Di solito il resto viene dimenticato.

Così Chris mi ha dato la sua Merchant ID e il numero a cui telefonano per le richieste. Sarei stato più contento se avessi po-

tuto fare qualche altra domanda su quante informazioni erano ottenibili dalla CreditChex. Però era meglio non forzare la buona sorte.

Era come avere un assegno in bianco sulla CreditChex. Adesso potevo chiamare per farmi dare le informazioni che volevo, senza nemmeno pagare per il servizio. Alla fine ho scoperto che il tipo della CreditChex era ben lieto di dirmi quel che volevo, cioè i due posti in cui il marito della mia cliente aveva fatto recente rischiesta di apertura di conto. Dove potevano essere finiti i soldi che cercava la sua tra poco ex moglie? Dove se non nelle banche che mi aveva elencato il tipo alla CreditChex?

Analizziamo l'attacco

L'intero attacco si basava su una tattica fondamentale dell'ingegneria sociale: ottenere informazioni che un dipendente della ditta ritiene innocue e invece non lo sono.

La prima impiegata ha confermato la terminologia esatta del numero di identificazione usato quando chiamano la CreditChex: la Merchant ID. La seconda ha fornito il numero di telefono per chiamare l'agenzia, e l'informazione cruciale, il numero di Merchant ID della banca. Alle due impiegate sembravano informazioni innocue. In fondo stavano pensando di parlare con uno della CreditChex, quindi che male c'era a rivelare il numero?

Adesso erano state poste le basi per la terza telefonata. Grace aveva tutto quel che gli serviva per telefonare alla CreditChex, spacciandosi per un responsabile di una banca cliente e chiedere semplicemente l'informazione che gli serviva.

Abile a sgraffignare l'informazione come un buon borsaiolo è capace di rubare il portafoglio, Grace aveva un talento allenato nell'interpretazione delle persone. Era inoltre al corrente della classica tattica di nascondere le richieste chiave tra quelle innocenti, e sapeva che una domanda personale avrebbe saggiato la disponibilità della seconda impiegata prima di chiederle con fare innocente il numero Merchant ID.

L'errore della prima impiegata che ha confermato la terminologia è quasi impossibile da evitare. È un'informazione tanto banale nel settore bancario da sembrare irrilevante, l'emblema dell'innocuità. Ma Chris, la seconda impiegata, non doveva dimostrarsi tanto disponibile a rispondere senza essere sicura che chi chiamava fosse chi sosteneva di essere. Come minimo doveva prendere numero e nome e richiamare, così se dopo saltavano fuori problemi poteva almeno sapere da dove aveva telefonato quel tale. In questo caso una chiamata del genere a-

vrebbe reso molto più difficile farsi passare per un dipendente della CreditChex.

Sarebbe stato ancora meglio chiamare la CreditChex usando un numero già presente (non quello fornito dall'interlocutore) per verificare che quella persona lavorasse dawero lì e che stessero facendo sul serio un controllo sui clienti. Però, dati gli impegni del mondo reale e la carenza di tempo che quasi tutti patiamo oggigiorno, è un po' eccessivo aspettarsi questo tipo di telefonate di verifica, a meno che un dipendente non sospetti un qualche genere di attacco.

> Una Merchant ID è analoga in questa situazione a una password. Se il personale della banca la trattasse come un PIN di Bancomat capirebbe meglio quanto è delicata come informazione. Nella vostra organizzazione c'è un codice interno o un numero che il personale non tratta con sufficiente attenzione?

LA TRAPPOLA DELL'INGEGNERE

È risaputo che le ditte di cacciatori di teste usano i metodi tipici dell'ingegneria sociale per reclutare talenti. Ecco un esempio di come può andare.

Alla fine del decennio scorso un'agenzia di collocamento non molto etica si accordò con un nuovo cliente, un'azienda che cercava ingegneri elettronici con esperienza nel settore telefonico. L'incaricato dell'agenzia era una signora dalla voce profonda e dai modi insinuanti che aveva imparato a far nascere la fiducia altrui e una certa intimità anche per telefono.

La brava donna optò per un'incursione ai danni di un fornitore di servizi di telefonia cellulare per vedere se riusciva a rintracciare qualche ingegnere disponibile a passare alla concorrenza. Non poteva certo chiamare il centralino per chiedere: "Posso parlare con qualcuno che abbia cinque anni di esperienza nel campo?". Invece, per motivi che diventeranno chiari tra poco, iniziò l'assalto ai talenti altrui cercando un'informazione che sembrava marginale, che i dipendenti potevano dare a chiunque la richiedesse.

La prima telefonata: centralinista

L'attaccante, sotto lo pseudonimo di Didi Sands, telefona alla sede del fornitore di servizi di telefonia mobile. La conversazione è andata circa così:

CENTRALINISTA: Buon pomeriggio, sono Marie. In cosa posso esserle utile?

DIDI: Può passarmi il settore trasporti?

R: Non so se ne abbiamo uno. Adesso guardo nell'elenco. Chi devo dire?

D: Didi.

R: Parla da qui o…

D: No, chiamo da fuori.

R: Didi chi?

D: Didi Sands. Avevo l'interno dei trasporti però me lo sono scordato.

R: Un attimo.

A questo punto, per sedare eventuali sospetti, **Didi** fa una domanda come se niente fosse, tanto per fare conversazione, per far capire che sa tutto, che è al corrente dell'andazzo.

D: Con che palazzo sto parlando? Lakeview o **Main** Place?

R: **Main** Place. (Pausa) il numero è 805 555 6469.

Per avere la scusa nel caso che la telefonata ai trasporti non le fornisca quanto cerca, **Didi** segnala che vuole parlare anche con l'ufficio Immobili. E così la centralinista le fornisce anche il secondo numero. Quando **Didi** chiede di passarle i trasporti la centralinista ci prova ma il numero risulta occupato.

A questo punto **Didi** domanda un ***terzo*** numero, i crediti esigibili, un ufficio sito in una struttura a Austin, nel Texas. L'altra le chiede di pazientare un momento e si sconnette. Forse sta riferendo alla sorveglianza che ha una telefonata sospetta e c'è qualcosa che non torna? Per nulla, e **Didi** non deve stare in ansia. Certo, è una scocciatura per la centralinista, ma come tante nella classica giornata di lavoro. Dopo circa un minuto l'altra torna in linea e passa **Didi** ai crediti.

Seconda telefonata: Peggy

La conversazione successiva è andata circa così:

PEGGY: Crediti, sono Peggy.

DIDI: Ciao, Peggy, sono **Didi** di Thousand Oaks.

P: Ciao, **Didi**.

D: Come va?

P: Bene.

Poi **Didi** usa un noto termine aziendale per quando devono caricare le spese sul bilancio di una specifica organizzazione o gruppo di lavoro.

D: Ne sono lieta. Senti, avrei una domanda. Come trovo l'ufficio spese di un dato settore?

P: Devi contattare l'analista di bilancio del dipartimento.

D: E sai chi è a Thousand Oaks, alla sede centrale? Sto cercando di compilare un modulo ma non so qual è l'ufficio giusto.

P: So solo che quando serve un numero dell'ufficio spese devi chiamare l'analista di bilancio.

D: Lì nel Texas avete un ufficio spese nel vostro settore?

P: **Sì,** ma non ci danno la lista completa.

D: Quante cifre ha l'ufficio spese? Per esempio, il tuo com'è?

P: Mah. Sei del 9WC o del SAT?

Didi non ha la minima idea di cosa significhi, ma non importa. Invece risponde:

D: 9WC.

P: Allora di solito è di quattro cifre. Da dove hai detto che chiami?

D: Dalla sede di Thousand Oaks.

P: Be', eccolo qua quello di Thousand Oaks. È 1A5N, N come **Nancy.**

Solo stando in linea abbastanza a lungo con una persona disponibile, **Didi** ha ottenuto il numero che le serviva, una di quelle informazioni che nessuno pensa di proteggere perché sembra priva di valore per un estraneo.

La terza telefonata: un utile numero sbagliato

Il prossimo passo di **Didi** consiste nello scambiare il numero dell'ufficio spese con qualcosa di valido, come se fosse un gettone al tavolo da gioco.

Inizia chiamando il settore immobili, fingendo di aver composto il numero sbagliato. Dopo avere esordito con "Mi dispiace di disturbare, ma..." sostiene di essere una dipendente che ha perso l'elenco interno e vuole sapere chi deve chiamare per ottenere una nuova copia. L'uomo al telefono risponde che non c'è più bisogno della obsoleta versione su carta essendo l'elenco reperibile nel sito intranet.

Quando **Didi** sostiene di preferire la copia su carta l'altro le consiglia di chiamare le pubblicazioni e senza essere richiesto, forse per tenere un po' di più al telefono quella signora sexy, controlla il numero e glielo comunica.

La quarta telefonata: Bart delle pubblicazioni

Alle pubblicazioni **Didi** parla con un certo Bart, a cui dice di essere di Thousand Oaks e di avere bisogno di una copia dell'elenco aziendale, e che la versione stampata sarebbe più pratica, anche se non è aggiornata. Quando Bart le dice che deve compi-

lare una richiesta da spedire a lui, Didi risponde che ha finito i moduli e avrebbe una gran fretta. Sarebbe tanto carino Bart da compilarne uno per lei? Quando lui accetta con eccessivo entusiasmo, Didi gli dà i particolari. Come indirizzo del finto cliente ha scribacchiato il numero di quella che gli ingegneri sociali chiamano la "mail drop", in questo caso una cassetta presso una specie di mail boxes dove la sua ditta ne tiene sempre in previsione di casi del genere.

Adesso le torna utile il precedente lavoro di spada: c'è qualcosa da pagare per la spedizione dell'elenco. Perfetto, Didi dà il codice dell'ufficio spese di Thousand Oaks: "1A5N, N come Nancy".

Qualche giorno dopo, quando arriva l'elenco aziendale, Didi scopre che è ancora più succulento del previsto. Non solo contiene nomi e numeri di telefono, ma riporta anche chi lavora per chi, l'intera struttura aziendale.

La signora dalla voce sensuale è pronta a fare le sue telefonate da cacciatrice di teste. Ha rubato l'informazione che le serviva per lanciare la campagna solo sfruttando la parlantina addestrata allo spasimo di ogni abile ingegnere sociale. Adesso è pronta per la vendemmia.

Analizziamo l'attacco

In questo esempio di ingegneria sociale Didi ha iniziato procurandosi i numeri di telefono di tre uffici della compagnia bersaglio. È stato facile perché i numeri che chiedeva non erano un segreto, soprattutto per il personale. Un ingegnere sociale impara presto a sembrare uno del giro, e Didi era molto brava in questo specifico esercizio. Uno dei numeri l'ha portata all'ufficio spese, di cui ha usato il codice per farsi inviare una copia dell'elenco dei dipendenti.

> Ogni frammento di informazione, come le tessere in un puzzle, in sé e per sé è privo di valore, però quando i pezzi vengono messi insieme otteniamo un'immagine chiara. In questo caso, l'immagine vista dall'ingegnere sociale è la struttura interna dell'azienda.

Quali sono stati i suoi principali strumenti di lavoro? Sembrare amichevole, usare il gergo aziendale e, con l'ultima vittima, sbattere le ciglia per telefono.

E un'altra arma ancora, un elemento essenziale meno facile da acquisire, la bravura nella manipolazione tipica dell'ingegnere sociale affinata con allenamenti intensivi e con le lezioni non scritte delle precedenti generazioni di furbi.

A parte i numeri interni e il codice dell'ufficio spese, quali altre informazioni apparentemente inutili possono risultare estremamente preziose per il vostro nemico?

La telefonata a Peter Abels

"Buongiorno, sono Tom della Parkhurst Travel. I suoi biglietti per San Francisco sono pronti. Vuole che li consegnamo noi o passa a prenderli?" chiede la voce all'altro capo del filo.

"San Francisco? Non devo andare a San Francisco," protesta Peter.

"Lei è Peter Abels?"

"Sì, ma non ho alcun viaggio in programma."

"Ehi, è proprio sicuro di non voler andare a San Francisco?" fa l'interlocutore con una risata cordiale.

"Se crede di poter convincere il mio capo…" ribatte Peter, stando al gioco.

"Mi sembra un errore. Sul nostro sistema abbiamo i documenti di viaggio sotto il numero di previdenza sociale. Forse qualcuno ha usato quello sbagliato. Qual è il suo?"

Peter fornisce senza discutere il suo Social Security Number (Ssn). E perché no? Compare su quasi tutti i documenti aziendali che compila, lo conoscono tanti colleghi, le risorse umane, l'ufficio paghe e naturalmente quello trasferte. Nessuno tratta il Ssn come se fosse un segreto. Che differenza può fare?

Non è difficile capire la risposta. Bastano un paio di informazioni per assumere una personalità credibile, per rubare l'identità di un altro. T'impossessi di un nome di dipendente, del suo numero di telefono e casomai per buona misura anche dei dati del suo direttore, e anche se non sei il massimo hai già più di quel che ti serve per sembrare verosimile al prossimo bersaglio che chiami.

Se ieri vi avesse telefonato una persona che diceva di essere di un altro reparto della vostra ditta dando una ragione plausibile e chiedendovi il vostro numero di matricola avreste detto di no?

A proposito, qual è?

La morale della storia è: non date alcuna informazione personale o interna alla ditta o identificativi a chicchessia, a meno che la voce non sia conosciuta e il richiedente sia autorizzato.

La vostra azienda deve far capire ai dipendenti quanto possa essere grave la gestione scorretta delle informazioni riservate. Una sensata politica di sicurezza delle informazioni unita a una preparazione adatta sensibilizzeranno in modo spettacolare la consapevolezza dei dipendenti riguardo la gestione delle informazioni interne. Una serie di misure sulla riservatezza dei dati vi aiuterà a mettere in atto i giusti controlli sulla rivelazione di informazioni. In sua assenza tutte le informazioni interne devono essere ritenute confidenziali fino a diverso ordine.

Assumete questi provvedimenti per proteggere la vostra impresa dal rilascio di informazioni apparentemente innocue:

- Il settore preposto alla protezione delle informazioni ha bisogno di una preparazione alla condotta che spieghi i metodi usati dagli ingegneri sociali. Un metodo sopra descritto prevede di ottenere informazioni apparentemente neutre e usarle come moneta di scambio per accattivarsi la vostra fiducia. Ogni impiegato deve capire che quando chi telefona è al corrente delle procedure interne, del gergo e degli elementi identificativi ciò non lo autentica in alcun modo né gli dà il diritto di essere informato. Chi telefona potrebbe essere un ex dipendente o un fornitore che è al corrente di questi dettagli. Quindi ogni grande azienda deve decidere un adatto metodo di autentica da usare quando i dipendenti interagiscono con individui che non conoscono di persona o tramite telefono.
- La persona o più persone che devono stilare una strategia sulla riservatezza dei dati devono analizzare i passaggi che possono essere usati per arrivare a un dipendente. Anche se non date mai il vostro codice di Bancomat, rivelate forse il fornitore che usate per sviluppare il software dell'azienda? Questa informazione potrebbe essere sfruttata da chi fingerà di avere un accesso legittimo alla rete aziendale?
- Certe volte basta conoscere la terminologia interna per sembrare autorevole e aggiornato. Spesso l'attaccante si basa su questo equivoco comune per raggirare le sue vittime. Per esempio, una

> Come dice una vecchia battuta: persino un paranoico totale ha qualche nemico. Dobbiamo dare per scontato che anche ogni impresa abbia dei nemici, gente che prende di mira le infrastrutture della rete per strappare i segreti aziendali. Non accettate di diventare una statistica dei crimini informatici, è venuta l'ora di approntare le difese necessarie applicando i controlli del caso tramite politiche e procedure sensate di sicurezza.

Merchant ID è un identificatore che l'ufficio preposto ai nuovi conti correnti di una banca usa disinvoltamente tutto il giorno, ma è equivalente a una password. Se ogni dipendente capisse la sua natura, cioè che può essere usato per autenticare chi fa una richiesta, lo tratterebbe con maggiore cautela.

- Nessuna azienda, be', almeno molto poche, rilascia i numeri diretti degli amministratori, però quasi tutte non hanno problemi a rivelare i numeri di telefono di tanti settori dell'organizzazione, soprattutto a una persona che è o sembra essere un dipendente. Possibile contromisura: instaurate una politica che proibisca di dare i numeri interni di dipendenti, fornitori, consulenti e awentizi. Ancor più importante, pensate a una procedura passo-dopo-passo per verificare se chi chiama per chiedere un numero di telefono è davvero un dipendente.
  I codici spese dei vari settori e uffici, oltre alle copie dell'elenco interno (che siano su carta, su dischetto o in intranet), sono frequenti bersagli degli ingegneri sociali.
  Ogni azienda ha bisogno di una politica scritta e chiara riguardo la rivelazione di questo genere di informazioni, compreso un registro per segnalare i casi in cui informazioni delicate siano state rivelate agli esterni.
- Informazioni come il numero di matricola del dipendente o il suo Ssn non dovrebbero essere usate da sole come autentica. Ogni dipendente deve essere preparato a verificare non solo l'identità del richiedente ma anche il suo accesso alle informazioni.
- Nei vostri security training ricordatevi di insegnare ai dipendenti questo comportamento: quando un estraneo fa una domanda o chiede un favore, negare sempre fino a quando la richiesta potrà essere verificata, poi, prima di cedere al desiderio naturale di dimostrarsi utile, seguire le procedure aziendali riguardo la verifica e rivelazione di informazioni riservate, non pubbliche. Questo atteggiamento può contrastare con la tendenza atavica ad aiutare gli altri, ma un po' di salutare paranoia può rivelarsi necessaria se non volete essere la prossima preda dell'ingegnere sociale.

Come hanno dimostrato le storie di questo capitolo, le informazioni apparentemente innocue possono essere la chiave giusta per carpire i segreti più preziosi della vostra azienda.

3.
L'attacco diretto: basta chiedere

Molti attacchi di ingegneria sociale sono piuttosto complessi, composti di più mosse grazie a una pianificazione accurata in cui si fondono manipolazione e competenza tecnologica.

Però trovo sempre stupefacente come spesso un ingegnere sociale "scafato" riesca a ottenere quel che vuole con un banale attacco diretto. Basta chiedere l'informazione che serve, come vedrete.

UNA MLAC "AL VOLO"

Volete sapere il numero di telefono riservato di una persona? Un ingegnere sociale può insegnarvi una mezza dozzina di modi (che troverete descritti in altre storie di queste pagine) ma forse l'opzione più semplice sta in una sola telefonata come questa.

Il numero, prego

L'attaccante ha composto il numero dell'azienda telefonica corrispondente al MLAC, acronimo che indica il Centro per l'assegnazione automatizzata delle linee. Alla signora che risponde dice: "Salve, sono Paul Anthony, sono un giuntatore cavi. Senta, una centralina dei terminali è appena andata a fuoco. I poliziotti sospettano che sia stato un matto che ha cercato di bruciare casa sua per riscuotere l'assicurazione e adesso io mi trovo qui da solo a cercare di riparare un intero terminale da 200 linee e mi serve una mano. Quali strutture operano al 6723 di South Main?".

In altri settori dell'azienda telefonica la persona interpellata sa-

prebbe che le informazioni sui numeri che non figurano nell'elenco possono essere rilasciate solo al personale autorizzato, ma il numero MLAC dovrebbe essere noto solo ai dipendenti della compagnia. Mentre non divulgherebbero mai informazioni al pubblico, nessuno di loro rifiuterebbe un aiutino a un collega alle prese con un compito tanto arduo. La donna sta male per Paul, anche lei ha avuto brutte giornate in ufficio e così infrange un tantino le regole per aiutare un collega alle prese con un problema rivelandogli tutti i numeri funzionanti assegnati a quell'indirizzo.

> Fa parte della natura umana la fiducia nel prossimo, soprattutto quando la richiesta sembra ragionevole. Gli ingegneri sociali approfittano di questo assioma per sfruttare le loro vittime e ottenere ciò che vogliono.

Analizziamo l'attacco

Come noterete a più riprese in queste storie, conoscere il gergo di un'azienda e la sua struttura, i vari uffici e settori, cosa fa e quali informazioni detiene ciascun dipartimento, fa parte del fondamentale bagaglio di trucchi dell'ingegnere sociale di successo.

UN GIOVANE IN FUGA

Un tale che chiameremo Frank Parsons è contumace da anni, ricercato dai federali per aver fatto parte negli anni sessanta di un gruppo clandestino contro la Guerra nel Vietnam. Quando è al ristorante sta sempre girato verso la porta, e ogni tanto si guarda alle spalle, un gesto sconcertante. Ogni tot anni trasloca da una città all'altra.

A un certo punto è arrivato in una città che non conosce e ha iniziato a cercare lavoro. Per uno come lui, abile al computer (e pure nell'ingegneria sociale, anche se questo non lo cita nelle richieste di impiego) trovare un buon lavoro non è mai un problema. A parte i periodi di recessione, le persone con competenze informatiche sono molto richieste e cadono sempre in piedi. Frank ha subito individuato un impiego ben pagato in una ricca struttura di assistenza malati poco lontano da dove abita.

Purtroppo, appena ha iniziato a districarsi nei moduli di domanda, ha trovato un ma: il datore di lavoro richiede la fedina penale del candidato, rilasciata dalla polizia di stato. Nella pila di scartoffie c'era anche il modulo per chiedere quel documento

con un quadratino per inserire un'impronta digitale. Anche se era solo quella dell'indice destro, se per caso avessero notato la concordanza con quella conservata nel database dell'FBI molto presto Frank avrebbe trovato lavoro, certo, ma alla mensa di un carcere federale.

Frank ha però pensato che forse, solo forse, poteva sfangarla. Chissà, può darsi che quello stato non mandi le impronte all'FBI. Come fare per saperlo?

Come? È un ingegnere sociale, no? Ecco che telefona alla polizia di stato. "Salve. Stiamo conducendo uno studio per conto del ministero della Giustizia e stiamo indagando quanto occorrerebbe per un nuovo sistema di identificazione delle impronte. Posso parlare con qualcuno che mi può aiutare?"

E quando l'esperto è arrivato al telefono gli ha fatto una serie di domande sui sistemi che usavano e su dove analizzavano e conservavano le impronte. Avevano problemi di macchinari? Erano collegati con il Centro nazionale informazioni sul crimine (NCIC) o soltanto con le strutture statali? I macchinari erano semplici da imparare a usare?

Sornione, è riuscito a infilare la domanda chiave.

La risposta è stata musica per le sue orecchie: no, non erano collegati al Centro nazionale ma solo all'Indice informazioni criminali (CII) dello stato.

Era quello che Frank voleva sapere. Lui non aveva trascorsi in quello stato perciò ha potuto presentare domanda, essere assunto e nessuno si è presentato un giorno alla sua scrivania dicendo: "Quei signori sono dell'FBI e vorrebbero parlare con te".

E a sentir lui si è dimostrato un impiegato modello.

> Gli astuti ladri di informazioni non hanno remore a telefonare a funzionari statali, federali o locali per aggiornarsi sulle procedure usate dai tutori dell'ordine, *e* con queste informazioni in saccoccia aggirano i vostri controlli standard di sicurezza.

Sulla *soglia*

Nonostante il mito dell'ufficio senza carta, le aziende continuano a stampare valanghe di fogli ogni giorno. Le informazioni su carta della vostra azienda possono essere vulnerabili anche se state usando tante precauzioni e il timbro di documento riservato. Ecco un aneddoto che vi dimostra come un ingegnere sociale riesca a ottenere i vostri documenti più segreti.

Manovra loop-around

Ogni anno l'azienda telefonica pubblica (o almeno pubblicava, essendo in libertà vigilata non posso domandarglielo) un volume chiamato "Elenco numeri collaudo", un documento di grande valore per i phreak, perché è pieno di numeri riservatissimi usati dai tecnici e affini per attività quali testare i tronchi principali o controllare i numeri che danno sempre occupato.

Uno di questi numeri test, conosciuto in gergo come "loop-around, era particolarmente utile, usato dai phreak per trovare altri come loro con cui parlare gratis. Inoltre, era anche un modo per dare un numero a cui far richiamare una banca, per esempio.

L'ingegnere sociale dà a un impiegato della banca un numero per raggiungerlo in ufficio, e quando il bancario richiama il phreak riceve la chiamata su un numero irrintracciabile.

Un "Elenco numeri collaudo" fornisce quindi un sacco di informazioni utili per qualsiasi phreak testosteronico e affamato di info. Perciò ogni anno, quando uscivano, i nuovi elenchi erano agognati da un sacco di giovanotti con l'hobby dell'esplorazione della rete telefonica.

> L'addestramento alla sicurezza rispetto alla politica aziendale per proteggere le informazioni utili dev'essere allargato a tutti i dipendenti, non solo a coloro che hanno accesso elettronico o fisico alla IT aziendale.

La trovata di Stevie

Naturalmente le compagnie telefoniche fanno sì che non sia facile averli: per questo i phreak devono dimostrarsi creativi. Come? Un giovane desideroso di possedere un volume del genere potrebbe recitare una scenetta di questo tipo.

Sul tardi di una calda serata d'autunno nella California meridionale un tale che chiamerò Stevie telefona alla sede centrale di una piccola azienda telefonica, all'edificio da cui corrono i cavi verso tutte le case e imprese dell'area coperta dal loro servizio.

Quando il centralinista di servizio risponde, Stevie dichiara di essere un collega del settore che stampa e distribuisce i materiali scritti. "Abbiamo il nuovo elenco dei numeri collaudo, ma per motivi di sicurezza non possiamo consegnarle la sua copia fino a quando non preleviamo la vecchia. E il ragazzo delle consegne è in ritardo. Se vuole lasciare la sua fuori dalla porta lui può passare dopo a prenderla e consegnare la nuova."

Il centralinista ignaro trova ragionevole questo comporta-

mento e fa esattamente come richiesto, lasciando sulla soglia del palazzo la sua copia dell'elenco sulla cui copertina è scritto in grandi lettere rosse "RISERVATO ALL'AZIENDA. QUANDO NON PIÙ UTILIZZATO, QUESTO DOCUMENTO DEVE ESSERE DISTRUTTO".

Mentre passa in macchina Stevie controlla con attenzione che non ci siano sbirri o guardie giurate appostati dietro gli alberi o tra le auto parcheggiate. Nessuno. Raccoglie disinvolto l'elenco e se ne va.

Ecco un altro esempio di quanto sia facile per l'ingegnere sociale ottenere quel che vuole seguendo il semplice principio del "basta chiedere".

In questi casi non vengono messi a repentaglio solo i beni della compagnia, ma anche i clienti dell'azienda.

Il lavoro come impiegato all'ufficio clienti comporta frustrazioni, risate e un sacco di errori inconsapevoli, alcuni dei quali possono avere conseguenze spiacevoli per i clienti dell'azienda.

La versione di Janie Acton

Janie Acton lavorava da tre anni in un cubicolo dei servizi alla clientela della Hometown Electric Power di Washington, ed era considerata un'ottima impiegata, intelligente e coscienziosa.

Era la settimana del Giorno del Ringraziamento quando arrivò quella telefonata. L'uomo che chiamava disse: "Sono Eduardo del reparto fatturazione. Ho in attesa una signora, la segretaria di un vicepresidente che chiede informazioni. Purtroppo non posso usare il mio computer. Ho ricevuto una e-mail da una ragazza delle risorse umane intestata 'ILOVEYOU' ma quando ho aperto l'allegato non sono più riuscito a usare la macchina. Un virus. Mi sono beccato uno stupido virus. Puoi cercarmi tu un'informazione cliente?"

"Certo," rispose Janie. "Ti è andato in bomba il computer? Terribile."

"Già."

Qui l'attaccante ha usato un'informazione ricavata dalle sue ricerche pregresse per sembrare più autentico. Avendo saputo che il dato che cercava era conservato nel cosiddetto Sistema informazioni fatturazione clienti, come lo chiamavano i dipendenti, chiese: "Puoi trovarmi un cliente sul SIFC?".

"Numero?"
"Non ce l'ho. Devi trovarlo in base al nome."
"Va bene. Qual è il nome?"
"Heather Marning." Mentre lui faceva lo spelling Janie digitava.
"Eccolo."
"Fantastico. Il servizio è attivo?"
"Ah-ah, è aperto."
"E il numero sarebbe?" chiese lui.
"Hai da scrivere?"
"Pronto."
"Il numero è BAZ6573NR7Q."
Lui lo rilesse, poi chiese: "E l'indirizzo?"
Janie glielo diede.
"Telefono?"
La gentile impiegata gli diede pure quello.
Il presunto Eduardo la ringraziò e appese. Janie passò alla telefonata seguente, e non ci pensò più.

Il progetto di ricerca di Art Sealy

Art Sealy aveva smesso di lavorare come redattore freelance per piccole case editrici quando aveva scoperto che poteva fare più soldi con le ricerche per scrittori e aziende. Capì presto che le sue tariffe salivano in proporzione a quanto l'incarico lo portava vicino al confine, spesso sfumato, tra legale e illegale. Senza nemmeno accorgersene divenne un ingegnere sociale che utilizzava tecniche familiari a ogni broker di informazioni, capendo di avere un talento innato per quella attività, dal momento che scopriva da solo trucchi che di solito gli ingegneri sociali devono imparare da altri. Dopo un po' superò il confine senza provare il minimo senso di colpa.

Mi ha contattato un tale che stava scrivendo un libro sull'amministrazione Nixon e cercava un "minatore di dati" per uno scoop su William E. Simon, che era stato ministro del Tesoro di Nixon. Simon era morto ma l'autore aveva il nome di una donna della sua squadra ed era abbastanza sicuro che abitasse nella capitale anche se non trovava l'indirizzo. Non aveva nemmeno il telefono registrato a nome suo, o almeno nessun numero sull'elenco. Fu per questo che il cliente mi chiamò, e io gli dissi che non c'era problema.
È il genere di incarico in cui bastano di solito un paio di telefonate se sai come fare. Qualsiasi azienda di servizio pubblico

> Mai pensare che gli attacchi degli ingegneri sociali debbano essere trucchi tanto complessi da essere individuabili prima della fine. Alcuni sono attacchi molto semplici, veri mordi e fuggi, nulla di più di un... be', basta chiedere.

fornisce informazioni del genere, per lo più dopo un paio di piccole bugie.

Mi piace cambiare tattica ogni volta, perché il lavoro resti interessante. "Tal dei Tali è in ufficio?" ha sempre funzionato, come anche "ho una persona in linea dall'ufficio del vicepresidente", che infatti mi venne utile in questo caso.

Devi affinare l'istinto, devi intuire quanto può essere disponibile la persona che hai all'altro capo del filo. Stavolta ho avuto fortuna con questa signora amichevole e gentile. Con una sola chiamata ho ottenuto indirizzo e numero di telefono. Missione compiuta.

Analizziamo l'attacco

Janie era sicura che l'informazione sul cliente fosse delicata, e non avrebbe mai discusso del suo conto con un altro cliente né dato informazioni personali al pubblico.

Però è chiaro che per quanti chiamano da dentro l'azienda vigano regole diverse. I colleghi giocano nella stessa squadra e quindi devono darsi una mano. Il tipo della fatturazione avrebbe verificato i dati da solo se non avesse avuto il computer in crisi per un virus, così lei è stata lieta di poter aiutare un compagno.

Art è arrivato poco per volta all'informazione chiave che cercava, ponendo domande su dettagli che non gli servivano come il numero dell'utenza. Eppure anche quello era un discreto ripiego: se l'impiegata si fosse insospettita, lui avrebbe richiamato con maggiori possibilità di successo perché conoscendo quel numero sarebbe parso più genuino al successivo passacarte.

Janie non immaginava che una persona potesse mentire per cose del genere, che l'interlocutore potesse anche non essere della fatturazione. Non dovete fargliene una colpa. Non era al corrente della regola di accertare sempre con chi stava parlando prima di discutere le informazioni contenute nella scheda di un cliente. Nessuno le aveva spiegato i pericoli di una telefonata da parte di uno come *Art.* Non apparteneva alla politica della ditta, non faceva parte del suo apprendistato e il suo direttore non gliene aveva mai fatto cenno.

Ecco un elemento da inserire nella vostra preparazione alla sicurezza: solo perché un chiamante o un visitatore conosce i nomi di qualcuno in ditta o il gergo aziendale non significa che è chi afferma di essere, né lo identifica come persona autorizzata a ricevere informazioni interne oppure all'accesso al vostro sistema informatico o alla rete.

L'addestramento alla sicurezza deve battere su un punto: nel dubbio verificare, verificare, verificare.

Una volta l'accesso alle informazioni di un'impresa era segno di rango. La manovalanza riforniva le caldaie, faceva andare le macchine, batteva le lettere e presentava rapporti, il capomastro o il direttore gli dicevano cosa fare, quando e come. Erano loro che sapevano quanti pezzi un operaio doveva produrne in un turno, e in quali colori e forme la fabbrica doveva sfornarne quella settimana, la prossima ed entro la fine del mese.

Gli operai gestivano le macchine, gli utensili e i materiali, i capi le informazioni. Un dipendente poteva solo ricevere l'informazione attinente al suo compito specifico.

Oggi il quadro è un po' diverso, non trovate? Molti operai usano un computer o una macchina computerizzata. Per una parte notevole della forza lavoro l'informazione critica scende fino al livello della loro scrivania perché possano operare. Nell'ambiente attuale quasi tutto quello che fanno i dipendenti coinvolge la gestione delle informazioni.

Ecco perché la politica di sicurezza di un'azienda dev'essere spalmata lungo tutta la struttura, indipendentemente dalla posizione. Tutti devono capire che non sono solo i capiufficio o i dirigenti a possedere l'informazione cercata da un attaccante. Oggi i lavoratori a tutti i livelli sono possibili bersagli, anche quelli che non usano i computer. Un novellino dei servizi per la clientela può essere l'anello debole che l'ingegnere sociale spezzerà per raggiungere l'obiettivo.

L'addestramento alla sicurezza e le relative politiche aziendali devono irrobustire quell'anello.

4.
Costruire la fiducia

Alcune di queste storie potrebbero indurvi a pensare che considero dei perfetti idioti tutti coloro che lavorano, pronti se non addirittura **smaniosi** di cedere ogni segreto che detengono. L'ingegnere sociale sa che non è vero. Perché i suoi attacchi sono tanto fortunati? Non perché la gente sia stupida o priva di buon senso. Come esseri umani siamo tutti vulnerabili ai raggiri perché tendiamo a fidarci immotivatamente se manipolati in una certa maniera.

L'ingegnere sociale anticipa sospetti e resistenze, ed è sempre pronto a ribaltare la sfiducia in fiducia. Se è in gamba programma l'attacco come se fosse una partita a scacchi, anticipando le domande che il bersaglio può porgli in modo da avere sempre la risposta pronta.

Una delle tecniche **più** classiche prevede di accattivarsi la fiducia della vittima. Come fa un truffatore a convincervi a fidarvi di lui? Credetemi, ci riesce.

FIDUCIA: LA CHIAVE DELL'INGANNO

Più l'ingegnere sociale riesce a **far** sembrare roba di tutti i giorni il suo contatto, **più** evita sospetti. Quando gli altri non hanno motivo di sospettare, per lui è facile guadagnare la loro fiducia.

Una volta ottenuta il ponte levatoio è abbassato e la porta del castello è spalancata per farlo entrare a prendere le informazioni che cerca.

La prima telefonata: Andrea Lopez

Andrea Lopez ha risposto al telefono del videonoleggio dove lavora, e un attimo dopo sta sorridendo: è sempre un piacere quando un cliente si prende il disturbo di dirle che è contento del servizio. Questo qua ha appena detto che ha avuto sempre ottime esperienze con questo negozio, tanto che vorrebbe mandare una lettera al titolare.

Quando gli chiede il nome del direttore e l'indirizzo, Andrea dice subito il nome, Tommy Allison, spiegando anche dove abita. Il cliente stava per appendere ma all'ultimo momento ha cambiato idea dicendo: "Vorrei scrivere anche alla sede centrale della vostra rete. Qual è il numero della vostra filiale?". Lei gli dà anche questa informazione, lui la ringrazia, aggiunge qualche complimento su quanto è stata gentile e la saluta.

"Una chiamata come questa fa passare più svelto il turno di lavoro. Come sarebbe bello se la gente fosse tutta così," pensa Andrea.

La seconda telefonata: Ginny

"Grazie per avere chiamato Studio Video. Sono Ginny, in cosa posso esserle utile?"

"Ciao, Ginny, sono Tommy Allison, titolare di Forest Park, negozio **863.** Abbiamo qui un cliente che vorrebbe noleggiare ***Rocky*** 5 ma abbiamo finito le copie. Puoi controllare se ne avete?" le domanda pimpante colui che chiama, con il tono di chi conosce Ginny da una vita.

Lei torna in linea dopo qualche secondo dicendo che ne hanno tre copie.

"Bene, adesso vedo se ha voglia di passare a prenderla. Grazie. Se hai bisogno di un favore basta che chiami e chiedi di Tommy, sarò lieto di fare il possibile."

Nelle due settimane seguenti Ginny riceve tre o quattro chiamate da Tommy per richieste varie. Sembrano domande legittime e lui suona sempre molto amichevole senza apparire assillante, aggiungendo ogni tanto due chiacchiere tipo "Hai sentito dell'incendio a Oak Park? Hanno chiuso un sacco di strade" eccetera. Quelle telefonate sono un piccolo diversivo dalla routine, e Ginny è sempre lieta di riceverle.

Un giorno Tommy telefona con l'aria sconvolta. "Avete per caso problemi con i computer?"

"No, perché?" ribatte Ginny.

"Un tipo è andato a sbattere contro un palo del telefono e il

tecnico dice che fino a quando non l'avranno sistemato un bel pezzo di città rimarrà senza telefono e Internet."

"Oh, no. Si è fatto male quel tipo?"

"L'hanno portato via in ambulanza. A proposito, avrei bisogno di una mano. C'è qui un vostro cliente che vorrebbe noleggiare *Il* padrino *II* ma non ha la tessera dietro. Potete controllare i dati?"

"Certo."

Tommy fornisce nome e indirizzo del cliente, che Ginny trova nel computer, dandogli il numero della tessera.

"Ha qualche pagamento in sospeso o in ritardo?" domanda Tommy.

"Non vedo nulla."

"Perfetto. Adesso segno a mano e inserisco dopo i dati appena i computer riprendono a marciare. Ah, vorrebbe addebitare sulla **Visa** che usa da voi, solo che non l'ha con sé. Mi dai il numero e la data di scadenza?"

Lei acconsente. Allora Tommy dice: "Grazie per l'aiuto. Ci sentiamo," e appende.

La versione di Doyle Lonnegan

Lonnegan non è il giovanotto che vorreste trovarvi davanti quando andate ad aprire la porta. È un museo ambulante di debiti di gioco, e fa anche qualche lavoretto di riscossione finché non lo sbilancia troppo. In questo caso gli hanno offerto una cifra considerevole per poco **più** di qualche telefonata a un **video**nolo. Si direbbe una passeggiata, solo che nessuno dei suoi "clienti" sa come condurre la truffa e gli serve uno con l'esperienza e il talento di Lonnegan.

La gente normale non firma assegni per coprire le puntate quando è sfortunata o incapace al tavolo da gioco. Lo sanno tutti. Allora perché questi miei amici continuavano a giocare con un imbroglione che non aveva il contante sul tavolo? Non chiedetelo a me. Forse erano a casa malati quando hanno distribuito il sale in zucca. Però sono amici, cosa posso farci?

Questo signore non aveva contante, così hanno accettato un assegno. Che roba. Dovevano portarlo al bancomat più vicino, ecco cosa. E invece no, un assegno. Per **3230** dollari.

Naturalmente è rimbalzato indietro. Che cosa vi aspettavate? Quindi mi hanno chiamato per sentire se potevo aiutarli. Di questi tempi non schiaccio **più** le dita della gente nella porta, del resto adesso ci sono metodi **più** raffinati. Gli ho detto: commissione 30%, vedo cosa posso fare. Loro mi danno nome e **indiriz**-

zo, e io vado al computer a controllare qual è il videonolo più vicino all'amico.

Non avevo una gran fretta. Quattro telefonate per lisciarmi la titolare e poi tombola, ho il suo numero di Visa.

Un altro amico mio possiede un topless bar. Per cinquanta verdoni può addebitare la perdita a carte del tizio sulla sua Visa come conto al bar. Che ci pensi l'imbroglione a spiegarlo a sua moglie. Credete che protesterà dicendo che non ha mai speso quei soldi? Pensateci un attimo. Sa che sappiamo chi è lui. E se riusciamo a ottenere il suo numero di carta di credito forse siamo capaci di peggio. Insomma, non c'è da stare in pensiero.

Analizziamo l'attacco

Le prime dhiamate di Tommy a Ginny servivano solo per ottenere la sua fiducia. Quando è arrivato il momento dell'attacco vero e proprio lei aveva la guardia abbassata e ha accettato Tommy per quel che diceva di essere, il titolare di un altro negozio della catena.

E perché no? Lo conosceva. Solo per telefono, è ovvio, però la loro era un'amicizia di lavoro, la base della fiducia. Una volta che lei l'ha accettato come figura credibile, come un negoziante della loro rete, la fiducia c'era già e il resto è stato una passeggiata.

> La tecnica dell'accattivarsi la fiducia è una delle tattiche più efficaci dell'ingegneria sociale. Dovete sempre domandarvi se conoscete sul serio la persona con cui state parlando. In certi rari casi potrebbe non rivelarsi chi sostiene di essere. Quindi dobbiamo imparare a osservare, a riflettere e a verificare l'identità.

VARIAZIONE SUL TEMA: CATTURA DELLA CARTA DI CREDITO

L'ottenimento della fiducia non richiede per forza una serie di telefonate alla vittima, come suggerito dall'aneddoto precedente. Mi ricordo un caso di cui sono stato testimone oculare dove sono bastati cinque minuti.

Papà, sorpresa

Una giorno ero seduto al tavolo di un ristorante con Henry e suo padre. Mentre conversavamo Henry ha iniziato a sgridare il padre perché diffondeva il numero di carta di credito come se fosse quello del telefono. "Capisco che devi darlo quando com-

pri qualcosa, però darlo a un negozio che lo infila nei suoi schedari, be', questo è davvero stupido."

"Lo faccio solo allo Studio Video," ha risposto il signor Conklin, citando l'ormai nota catena di videonoleggio. "Però controllo la Visa tutti i mesi e se ci fossero addebiti falsi me ne accorgerei."

"Certo, ma quando hanno il tuo numero è facile rubarlo."

"Intendi un dipendente disonesto?"

"No, tutti, non solo un dipendente."

"Che fesseria."

"Adesso chiamo e li convinco a darmi il tuo numero di Visa," ha ribattuto Henry.

"Non ce la farai **mai.**"

"In cinque minuti, qui, senza nemmeno alzarmi dal tavolo."

Il signor Conklin aveva l'aria di essere estremamente sicuro del fatto suo ma cercava di non darlo troppo a vedere. "Ripeto che non sai cosa dici. Se ci riesci questo è tuo," ha borbottato, piazzando sul tavolo un biglietto da cinquanta dollari.

"Papà, non voglio i tuoi soldi."

Henry ha estratto il cellulare, ha chiesto a suo padre in quale negozio andava e ha chiamato il servizio informazioni abbonati, anche per avere il telefono del vicino negozio di Sherman Oaks.

Ha poi chiamato in quest'ultimo sfruttando più o meno la tattica descritta nella storia precedente per ottenere nome e numero di telefono del titolare.

Poi ha telefonato alla filiale dove era socio suo padre, usando il vecchio trucco di fingersi titolare di un'altra sede e dando il numero del negozio che aveva appena appreso, per finire con la medesima scusa. "Oggi funzionano i vostri computer? I nostri non vanno tanto bene." Ha ascoltato la risposta e ha detto: "Senti, c'è qui un vostro cliente che vorrebbe noleggiare un video ma abbiamo i computer in tilt. Puoi controllare la sua tessera e verificare che sia vostro cliente?"

Henry ha dato il nome di suo padre poi, con un lieve cambiamento di tattica, ha chiesto di sapere numero di tessera, indirizzo, numero di telefono e data di apertura del conto. Infine: "Senti, ho una gran fila qui alla cassa. Mi dici anche numero e data di scadenza della carta di credito?".

Ha tenuto il telefono accostato all'orecchio con una mano mentre scriveva su un tovagliolo di carta con l'altra. Finita la telefonata, ha fatto scivolare il tovagliolo sotto il naso del padre, che l'ha letto a bocca aperta. Il poveretto era sconvolto, tutto il suo sistema di fiducia era appena finito nelle fogne.

Analizziamo l'attacco

Pensate adesso a come vi comportate quando qualcuno che non conoscete vi chiede qualcosa. Se arriva alla porta un estraneo tutto stracciato non lo fate entrare, se invece è ben vestito, con le scarpe lustre, i capelli in ordine, modi educati e un sorriso sulle labbra sarete meno sospettosi. Forse è un serial killer, però siete disposti a fidarvi di lui perché sembra normale e non brandisce un coltellaccio.

Meno evidente è il fatto che giudichiamo alla stessa stregua la gente al telefono. Questo tipo ha l'aria di volermi vendere qualcosa? È amichevole ed estroverso oppure intuisco ostilità o ansia? Parla come una persona istruita? Noi soppesiamo queste cose e forse una decina d'altre in modo inconscio, in un lampo, spesso nei primissimi istanti di conversazione.

> È naturale ritenere improbabile un inganno in una data transazione, salvo che non abbiate ragione di credere altrimenti. Noi soppesiamo i rischi e poi concediamo spesso alla gente il beneficio del dubbio. Di regola, la gente civile si comporta così... almeno la gente civile che non è mai stata truffata o manipolata o derubata di grosse cifre.
> Quando eravate piccoli, i vostri genitori vi insegnavano a non fidarsi degli estranei. Forse dovremmo tenere presente questo secolare principio nei posti di lavoro odierni.

Al lavoro la gente ci pone di continuo delle domande. Hai l'indirizzo e-mail di questo tizio? Dov'è l'ultima versione dell'elenco clienti? Chi è il responsabile di questa parte del progetto? Ti prego, mandami l'ultimo aggiornamento del progetto. Mi servirebbe la nuova versione del codice sorgente.

Guarda un po': certe volte quelli che fanno richieste del genere sono colleghi che non conoscete di persona, gente che lavora in un altro ramo dell'azienda o almeno sostiene di farlo. Ma se l'informazione che danno quadra e sembrano essere al corrente delle procedure ("Marianne ha detto..."; "È nel server K-16…"; "…revisione 26 dei nuovi piani del prodotto") allora allarghiamo la cerchia della fiducia fino a loro e concediamo tutti contenti quel che chiedono.

Certo, possiamo avere un'indecisione, chiederci come mai uno dell'impianto di Dallas ha bisogno di vedere i nuovi piani del prodotto, perciò gli facciamo un altro paio di domande. Se le risposte sono sensate e i modi rassicuranti, allora abbassiamo la guardia, torniamo alla nostra naturale predisposizione fiduciosa e facciamo (entro certi limiti) il possibile per soddisfarlo.

E non pensate per un solo momento che l'attaccante prenda di mira soltanto quelli che usano il sistema informatico dell'a-

zienda. E quello della posta? "Mi puoi fare un piacerino? Infilami questo nella sacca delle consegne interne." L'addetto alla posta può forse sapere che contiene un dischetto con un programmino speciale per la segretaria dell'arnministratore delegato? D'ora in poi l'attaccante avrà una sua copia privata delle e-mai1 del capo. Uau! Può succedere anche da voi? La risposta è: sì.

IL CELLULARE DA UN CENTESIMO

Molta gente si guarda intorno in cerca di meglio. Gli ingegneri sociali no, loro trovano la maniera di migliorare quel che hanno a disposizione. Per esempio, certe volte un'azienda lancia una campagna promozionale talmente buona che abboccano tutti, mentre l'ingegnere sociale esamina sempre l'offerta chiedendosi come approfittare ulteriormente della situazione.

Non molto tempo fa una compagnia nazionale di telefonia cellulare lanciò una grande promozione in cui offriva un telefonino nuovo di zecca per un centesimo a chiunque firmava uno dei loro contratti.

Tanta gente ha scoperto troppo tardi che ci sono numerose ottime domande che l'acquirente assennato dovrebbe sempre porre prima di firmare uno di questi piani per i cellulari: se il servizio è analogico, digitale o misto, il numero di minuti a tutte le ore che puoi sfruttare in un mese, se sono comprese le spese di roaming... eccetera eccetera. È soprattutto importante capire subito i termini del contratto, per quanti mesi o anni sarete vincolati.

Immaginatevi un ingegnere sociale di Filadelfia interessato a un telefonino a basso prezzo offerto alla firma da un'azienda di telefonia cellulare, però non gli garba il contratto accluso. Non c'è problema. Ecco come può gestire la situazione.

La prima telefonata: Ted

Per cominciare l'ingegnere sociale chiama un negozio di una catena di elettrodomestici sulla West Girard.

"Electron City. Sono Ted."

"Buongiorno, Ted, sono Adam. Senta, qualche sera fa ho parlato con un commesso per un cellulare. Ho detto che avrei richiamato appena deciso il genere di contratto, ma mi sono scordato come si chiama. Chi è quello che fa il turno serale in quel reparto?"

"Sono in parecchi. Era William?"

"Non ne sono sicuro. Che tipo è?"
"Alto. Abbastanza magro."
"Direi che è lui. E come fa di cognome?"
"Hadley. H-A-D-L-E-Y."
"Sì, mi sembra lui. Quando lo trovo?"
"Non so i suoi orari questa settimana, però quelli della sera arrivano verso le cinque."
"Perfetto. Allora provo stasera. Grazie, Ted."

La seconda telefonata: Katie

La seconda chiamata è a un negozio della stessa catena sulla North Broad Street.
"Pronto, Electron City. Sono Katie. Posso esserle utile?"
"Ciao, Katie. Sono William Hadley, del negozio sulla West Girard. Come va oggi?"
"Un po' a rilento. Che mi dici?"
"Ho un cliente qui per quel contratto con il telefono a un cent. Hai capito quale?"
"Certo. Ne ho venduti un paio la settimana scorsa."
"Hai ancora qualcuno di quegli apparecchi?"
"Un sacco."
"Perfetto. Perché ne ho appena venduto uno a un cliente che ha firmato il contratto. Però quando ho controllato in magazzino ho visto che non me ne sono rimasti, e adesso sono in imbarazzo. Puoi farmi un favore? Lo mando da te a ritirarne uno. Puoi venderglielo per un cent e fargli la ricevuta? Dovrebbe richiamarmi quando ha il telefono così gli dico come programmarlo."
"Certo. Mandamelo pure."
"Bene. Si chiama Ted, Ted Yancy."
Quando il tale che si fa chiamare Ted Yancy si fa vivo al negozio della North Broad Katie gli compila la ricevuta e gli vende il telefonino per un centesimo, come le ha chiesto di fare il "collega". Ha abboccato all'amo, lenza e tutto.
Quando è ora di pagare il cliente non ha spiccioli in tasca, così pesca nella ciotola dei penny presso la cassa, ne prende uno e lo dà alla ragazza al banco. In quel modo ottiene il telefono senza nemmeno sganciare il centesimo.
Adesso è libero di rivolgersi a un'altra compagnia che usi lo stesso modello per scegliere il contratto che preferisce, possibilmente mensile e senza impegni.

Analizziamo l'attacco

È naturale che le persone siano più malleabili con chi sostiene di essere un collega e conosca le procedure e il gergo dell'azienda. L'ingegnere sociale del precedente esempio se n'è approfittato scoprendo i dettagli di una promozione, spacciandosi per un dipendente della catena e chiedendo un favore a un'altra filiale. Succede spesso tra le varie sedi delle catene di negozi e tra i vari uffici di un'azienda, laddove le persone sono fisicamente separate e trattano con colleghi che di regola non conoscono direttamente.

Spesso non ci si sofferma a pensare ai materiali che la propria organizzazione mette a disposizione in Rete. Per le mie trasmissioni settimanali su KFI Talk Radio di Los Angeles, il produttore ha fatto una ricerca in Rete trovando la copia di un manuale di istruzioni per accedere al database del Centro nazionale informazioni sul crimine, poi ha trovato il manuale vero e proprio, un documento scottante che dà ogni indicazione su come ricavare informazioni dal database dell'FBI sui reati.

Si tratta di un testo pensato per le strutture di polizia che specifica le formattazioni e i codici necessari per recuperare dati su criminali e reati dall'archivio nazionale. Le agenzie di tutto il paese possono setacciare lo stesso archivio per risolvere i delitti nella propria giurisdizione. Quel manuale contiene i codici usati nel database per segnalare qualsiasi dettaglio, dai diversi tipi di tatuaggio agli scafi delle barche fino al taglio di soldi e titoli rubati.

Chiunque abbia accesso a quel testo può apprendere la sintassi e i comandi necessari per estrarre queste informazioni, poi, seguendo le istruzioni della guida-procedure, con un minimo di coraggio può ottenere i dati dall'archivio informatico. Inoltre, il manuale contiene i numeri di telefono da chiamare per ottenere assistenza nell'utilizzo del sistema. Potreste avere testi del genere, che offrono codici prodotto o aiutano a recuperare informazioni delicate, anche nella vostra azienda.

Penso che l'FBI non abbia mai scoperto che il suo manuale supersegreto pieno di istruzioni è disponibile a cani e porci in Rete, e non credo che sarebbero molto lieti di apprenderlo. Una copia è stata messa in Rete da un dicastero locale dell'Oregon, l'altra da una polizia del Texas. Perché? Devono aver pensato che non avesse un valore particolare e che metterlo in Rete non recasse danno. Forse l'hanno postato in intranet per utilizzo interno, senza capire che in quel modo le informazioni erano a di-

sposizione di chiunque in Internet avesse accesso a un discreto motore di ricerca come Google, compresi ficcanaso qualsiasi, poliziotti in erba, hacker e boss della malavita organizzata.

Inserirsi nel sistema

Il principio è sempre quello: dato che l'ingegnere sociale sa come accedere a specifici database e applicativi, oppure conosce i nomi dei server di un'azienda o roba del genere, appare più credibile. La credibilità porta alla fiducia.

Quando un ingegnere sociale è a conoscenza dei codici gli sarà facile ottenere le informazioni di cui necessita. In questo esempio comincia con il telefonare a un impiegato dell'ufficio telescriventi della locale polizia di stato, per porre una domanda su un codice del manuale, per esempio quello sulle lesioni gravi. Può dire qualcosa tipo: "Quando faccio una ricerca OFF presso l'NCIC ottengo sempre errore di sistema. Succede anche a voi? Può provare per me?". O forse racconta che stava cercando di aprire un file ricercati.

L'impiegata all'altro capo del filo capisce al volo che l'interlocutore è al corrente delle procedure operative e delle ricerche sul database NCIC. Chi altri se non una persona addestrata a usare l'NCIC potrebbe conoscere queste procedure?

Quando l'impiegata conferma che il suo sistema funziona alla perfezione, la conversazione procede più o meno così.

"Mi servirebbe un piccolo favore."

"Che cosa cerca?"

"Vorrei che desse il comando OFF su Reardon, Martin, data di nascita 18/10/66."

"Sosh?" (In gergo è il numero della previdenza sociale, Ssn.)

"700-14-7435."

Dopo aver controllato, la donna risponde: "Ha un 2602".

Adesso l'attaccante deve solo guardare l'NCIC in rete per scoprire il significato del numero: quel tale è pregiudicato per truffa.

Analizziamo l'attacco

Un ingegnere sociale in gamba non si ferma un attimo a scervellarsi su come fare a entrare di soppiatto nel database NCIC. Perché mai, quando una semplice chiamata alla polizia locale e qualche parolina gentile in modo da passare per un addetto ai lavori bastano a ottenere le informazioni che cerca? La prossima volta chiamerà una struttura diversa usando il medesimo pretesto.

Forse vi chiederete se non era rischioso telefonare a un dipartimento di polizia o all'ufficio dello sceriffo o a un agente della stradale. Non ha corso un grosso rischio?

La risposta è... no, e per un motivo ben preciso. I poliziotti, come i militari, hanno inculcato sin dal primo giorno in accademia il rispetto per i superiori. Se l'ingegnere sociale si fa passare per un tenente o un sergente, comunque più alto in grado della persona con cui parla, la vittima sarà ammorbidita dall'addestramento che impone di non fare domande ai superiori. Insomma, il grado ha i suoi privilegi, soprattutto quello di non sentirsi chiedere troppe cose dai sottoposti.

Ma non crediate che polizie varie ed esercito siano gli unici posti in cui l'ingegnere sociale può usare il grado. Spesso sfrutta per il suo attacco la posizione e l'autorità anche nella gerarchia aziendale, come dimostrano tante storie presentate su queste pagine.

PREVENIAMO GLI ATTACCHI

Tutti devono essere al corrente del modus operandi dell'ingegnere sociale: raccogliere più informazioni possibili sul bersaglio e poi sfruttarle per accattivarsi la fiducia in quanto persona appartenente al giro. E alla fine colpire alla giugulare!

Quali sono le misure che la vostra organizzazione può assumere per ridurre le probabilità che gli ingegneri sociali possano approfittarsi dell'istinto naturale dei vostri dipendenti a fidarsi delle persone? Ecco qualche consiglio.

Proteggere i clienti

In questa era elettronica tante aziende che vendono al dettaglio registrano le carte di credito. Ci sono motivi validi per farlo: per esempio, risparmia al cliente l'incomodo di fornire informazioni ogni volta che entra nel negozio o nel sito web per fare un acquisto. Però è una pratica che deve essere scoraggiata.

Se proprio dovete tenere in archivio i numeri di carta di credito, la procedura dev'essere accompagnata da contromisure che superino la semplice cifratura o un controllo dell'accesso. I dipendenti devono essere abituati a riconoscere al volo i trucchi degli ingegneri sociali quali quelli discussi in questo capitolo. Il collega che non avete mai visto di persona ma che è diventato un amico telefonico può anche non essere chi sostiene di essere. Forse non ha l'autorizzazione ad accedere a certe informazioni sulla clientela, perché forse non lavora nemmeno per la vostra stessa ditta.

Fidarsi con senno

Non sono soltanto coloro che hanno accesso a informazioni ovviamente delicate, i tecnici informatici, quelli della ricerca e sviluppo eccetera, che devono stare sempre in guardia contro le intrusioni. Quasi tutti i membri della vostra organizzazione devono essere addestrati a proteggere l'impresa dallo spionaggio industriale e dai ladri di informazioni.

Tanto per gettare le basi, iniziate con un'analisi delle informazioni chiave in tutta l'azienda, cercando separatamente ogni dato prezioso, delicato o critico e chiedendovi quali metodi un intruso potebbe usare per comprometterli tramite tattiche di ingegneria sociale. La preparazione adeguata per coloro che hanno accesso riservato a tali informazioni dovrebbe essere plasmata attorno alle risposte a questi interrogativi.

Fate in modo che il dipendente drizzi le orecchie quando un tizio che non si conosce di persona richiede informazioni o materiale, oppure domanda di eseguire qualcosa al computer. Se dessi questa informazione al mio peggiore nemico potrebbe essere usata per danneggiare me o la mia azienda? Comprendo appieno gli effetti potenziali delle operazioni che mi si chiede di compiere al computer?

Non vogliamo vivere nel sospetto di ogni persona che incontriamo, però più siamo fiduciosi più è probabile che il prossimo ingegnere sociale arrivato in zona possa convincerci a rivelare informazioni riservate della ditta.

Che cosa deve comparire sulla vostra intranet?

Una parte della vostra intranet può essere aperta all'esterno, altre limitate ai dipendenti. La vostra azienda è sempre pronta a verificare che le informazioni riservate non siano a disposizione di un utente da cui vorreste proteggerle? Quand'è stata l'ultima volta che uno della vostra organizzazione ha controllato per vedere se le informazioni delicate sulla vostra intranet erano inavvertitamente disponibili nelle aree di pubblico accesso del vostro sito web?

Se la vostra azienda utilizza dei server proxy come intermediari per proteggersi dalle minacce elettroniche, questi server sono stati controllati di recente per essere sicuri che fossero configurati nel modo giusto?

Anzi, qualcuno ha ***mai*** controllato la sicurezza della vostra intranet?

5.

"Posso aiutarla?"

Siamo tutti molto grati quando siamo assillati da un problema e una persona competente, abile e disponibile si offre di darci una mano. L'ingegnere sociale lo sa, e sa anche come approfittarsene.

Sa anche come causare quel vostro problema... poi ottenere la vostra gratitudine appena ve lo risolve... e alla fine giocare sulla gratitudine per estrarre informazioni e ottenere un piccolo favore da voi, lasciando la vostra azienda (oppure voi individualmente) in condizioni ben peggiori rispetto a prima dell'incontro. E forse non saprete nemmeno di aver perso qualcosa di prezioso.

Ecco alcune maniere classiche in cui gli ingegneri sociali si propongono di "aiutare".

L'INOPEROSITÀ DELLA RETE

Giorno/Ora: Lunedì 12 febbraio, 15:25
Luogo: Uffici della Starboard Shipbuilding

La prima telefonata: Tom DeLay

"Tom DeLay, contabilità."

"Ehi, Tom, sono Eddie Martin dell'assistenza. Stiamo cercando di risolvere i problemi della rete informatica. Sai se qualcuno del tuo gruppo ha problemi a restare in linea?"

"Non che io sappia."

"E tu non hai problemi?"

"No, tutto bene."

"Perfetto. Senti, stiamo telefonando alle persone che potrebbero essere colpite per sapere se vi cade la connessione."

"Suona poco allegro. Credete che potrebbe succedere?"
"Speriamo di no, ma tu chiama se succede. D'accordo?"
"Contaci."
"Immagino che un problema alla connessione sarebbe un bel guaio per te…"
"Puoi *scommetterci."*
"...perciò mentre noi ci diamo da fare ti do il mio numero di cellulare, così puoi raggiungermi direttamente se hai bisogno."
"Magnifico. Dimmi."
"555 867 5309."
"555 867 5309. Scritto. Grazie. Come hai detto che ti chiami?"
"Eddie. Senti, un'altra cosa. Dovrei sapere a che port number è collegato il tuo computer. Dai un'occhiata per vedere se c'è un adesivo con su scritto qualcosa tipo 'numero porta'."
"Resta in linea... No, non vedo niente del genere."
"Bene, allora, riconosci il cavo della rete sul retro del computer?"
"Certo."
"Vedi dove è attaccato e se c'è un'etichetta sullo spinotto."
"Un secondo. Sì, aspetta, devo chinarmi per leggere. Sì... dice Port **6** barra **47.**"
"Ottimo. Risulta anche a noi, ma è sempre meglio controllare."

La seconda telefonata: il tipo *dell'IT*

Due giorni dopo arriva una chiamata alla centrale operativa della rete della medesima ditta.
"Salve, sono Bob. Mi trovo nell'ufficio di Tom DeLay alla contabilità e stiamo cercando di risolvere un problema di cavi. Dovete disabilitarmi la porta **6/47."**
Il tipo dell'IT dice che sarà fatto tra qualche minuto, e di fargli sapere quando deve riabilitare.

La terza telefonata: aiuto dal nemico

Circa un'ora dopo, il tipo che si fa chiamare Eddie Martin sta facendo spese in un negozio di elettrodomestici quando squilla il suo telefonino. Allorché controlla vede che la chiamata viene dalla Starboard, perciò corre in un angolino riparato prima di rispondere.
"Assistenza, Eddie."
"Oh, ciao, Eddie. Sento un'eco. Dove sei?"
"Sono in un ripostiglio cavi. Chi è?"

"Sono Tom DeLay. Ragazzi, come sono contento di averti trovato. Ricordi che mi hai chiamato l'altro giorno? La mia connessione alla rete è saltata come avevi previsto, e adesso sono nel panico."

"Già, ne abbiamo parecchi in questo momento. Dovremmo risolvere la cosa entro oggi. Va bene?"

"NO! Accidenti, sarò in ritardissimo. Non potete fare di meglio?"

"Hai molta fretta?"

"Per adesso posso fare altre cose. È possibile che risolviate il tutto in mezz'ora?"

"MEZZ'ORA! Chiedi niente. Senti, mollo quel che sto facendo e vedo se posso aiutarti."

"Te ne sono molto grato, Eddie."

La quarta telefonata: beccato!

Quarantacinque minuti dopo...
"Torn? Sono Eddie. Prova la connessione."
Dopo qualche secondo:
"Perfetto, funziona. Fantastico."
"Sono lieto di esserti stato utile."
"Sì, grazie mille."

"Se vuoi essere sicuro che non vada di nuovo in panne ci sono dei programmi che puoi usare. Bastano un paio di minuti."

"Non è il momento migliore."

"Capisco... però ci risparmierebbe grossi grattacapi la prossima volta che succede."

"Be'... se sono solo pochi minuti."

"Adesso ti spiego..."

Poi Eddie gli fa scaricare una piccola applicazione da un sito web. Una volta che il programma è stato scaricato gli dice di farci sopra un doppio clic. L'altro prova, ma riferisce che non funziona, non succede nulla.

"Che palle. Dev'essere qualcosa nel programma. Sbarazziamocene, lo facciamo un'altra volta." E così Eddie fa cancellare a Tom il programma che in quel modo non potrà essere recuperato.

Tempo totale, 12 minuti.

La versione dell'attaccante

Bobby Wallace ha sempre trovato ridicolo un buon incarico come questo con il cliente che fa l'indiano sulla domanda non formulata ma owia del motivo per cui vuole quell'informazione.

In questo caso gli venivano in mente solo due ragioni. Forse il cliente rappresentava una struttura interessata ad acquisire la ditta bersaglio, la Starboard Shipbuilding, di cui voleva verificare la situazione finanziaria, soprattutto la roba che il bersaglio poteva tenere nascosta a un potenziale compratore. Oppure rappresentava alcuni investitori che sospettavano qualcosa di sporco su come venivano gestiti i soldi e volevano sapere se qualche dirigente ficcava le mani nel vaso della marmellata. O forse il cliente non voleva dirgli il vero motivo perché se Bobby avesse saputo quanto era preziosa l'informazione avrebbe chiesto altri soldi per il lavoro.

Ci sono tanti modi di rubare i documenti più segreti di un'azienda. Bobby ha passato qualche giorno a vagliare le varie possibilità e fare .qualche controllo prima di decidere un piano d'azione, poi ha scelto quello che prevedeva una tattica che adora, in cui è il bersaglio a chiedere aiuto all'aggressore.

Tanto per cominciare, compra un telefono da 39,95 dollari in un negozio e chiama il tizio che ha scelto come bersaglio facendosi passare per uno dell'assistenza informatica della ditta e mettendo le cose in modo che l'amico chiami il suo cellulare ogni volta che ha un problema con la connessione alla rete aziendale.

Lascia passare due giorni per non essere troppo prevedibile, poi chiama la centrale operativa della rete dell'azienda e sostiene che sta risolvendo un problema per Tom, il bersaglio, chiedendo di disabilitare la sua connessione. Sa che è questa la parte più problematica, in tante aziende l'assistenza è in stretto contatto con quel centro, anzi, spesso fa parte della struttura IT. Invece la persona con cui parla tratta la chiamata come se fosse routine, non chiede il nome del tecnico che in teoria sta risolvendo il problema e accetta di disabilitare la porta di rete del bersaglio. A quel punto Tom rimane totalmente isolato dall'intranet, non può recuperare file dal server, scambiarli con i colleghi, scaricare la posta o anche mandare pagine alla stampante. Nel mondo di oggi equivale a vivere in una caverna.

Come previsto, il telefono suona pochi minuti dopo. Ovviamente Bobby fa in modo di sembrare entusiasta di aiutare il povero "collega" nei guai e chiama il centro per far riabilitare la connessione. Alla fine risente la vittima convincendola un'altra volta. Si basa sul fatto che l'altro si sentirebbe in colpa dicendogli di no dopo che Bobby gli ha fatto un favore. Così Tom accetta di scaricare quel programmino nel suo computer.

Ovviamente quel che ha accettato non è quel che sembrava. Il programmino che doveva impedire alla sua connessione di andare in tilt era in realtà un "Trojan horse" (cavallo di Troia), un'ap-

plicazione che fa al suo terminale quello che fece il mitico cavallo dei greci, cioè far entrare il nemico dentro le mura. Tom ha segnalato che non è successo nulla quando ha fatto doppio clic sull'icona, ma in realtà a sua insaputa la piccola applicazione stava installando un programma invisibile che avrebbe consentito all'infiltratore l'accesso nascosto alla macchina di Tom.

Adesso, con il programma in funzione, Bobby ha il controllo completo del computer, una cosiddetta *remote command shell,* una shell di comandi remota. Quando accede al computer di Tom può cercare i file più interessanti e copiarli, poi con comodo esaminarli in cerca delle informazioni che vogliono i suoi clienti.

E non è tutto qui. Può tornare quando vuole a controllare i messaggi di posta elettronica e i memorandum riservati della dirigenza, awiando una ricerca delle parole che possono segnalare frammenti interessanti di informazione.

Subito dopo aver convinto il suo bersaglio a installare il cavallo di Troia ha gettato il cellulare in un cassonetto, ricordandosi di cancellare la memoria ed estrarre la batteria. L'ultima cosa che vuole è che qualcuno chiami quel numero per sbaglio e il telefono inizi a squillare!

Analizziamo l'attacco

L'attaccante tesse una tela per convincere il bersaglio di avere un problema che in realtà non esiste, o in questo caso un problema che non si è ancora verificato ma che l'attaccante sa che si presenterà perché sarà lui a provocarlo, per farsi poi vivo come la persona in possesso della soluzione.

Questo genere di attacco è quanto mai soddisfacente. Grazie al seme piantato in precedenza, appena il bersaglio scopre di avere un problema fa di persona la chiamata d'aiuto. L'altro deve solo stare ad aspettare che suoni il telefono, una tattica simpaticamente nota nel giro come "ingegneria sociale inversa" (reverse social engineering). L'attaccante che riesce a farsi telefonare dal bersaglio diventa immediatamente credibile: se telefono a un tale che ritengo lavorare all'assistenza non gli chiederò di dimostrare chi è. A questo punto l'attaccante ce l'ha fatta.

Se un estraneo vi fa un favore e poi vi chiede un controfavore non ricambiate senza aver riflettuto attentamente su che cosa vi sta domandando.

In un raggiro del genere l'ingegnere sociale cerca di scegliere una vittima che abbia una conoscenza limitata dei computer. Più l'altro ne sa più è probabile che si insospettisca o capisca di essere manipolato. Quello che ogni tanto chiamo il dipendente

informaticamente svantaggiato, colui che sa poco o nulla di tecnologia e procedure, è il più pronto a obbedire. È più probabile che cada nella trappola dello "scarica questo programmino" perché non immagina il danno potenziale che un programma può infliggere. Probabilmente non capirà che quell'informazione sta mettendo a repentaglio la rete informatica.

UN AIUTINO PER LA NEOASSUNTA

I nuovi assunti sono una ghiotta preda per gli attaccanti. Non conoscono ancora molta gente, non conoscono le procedure e gli obblighi della ditta. E per offrire una buona prima impressione sono ansiosi di dimostrarsi collaborativi e pronti a rispondere.

Andrea, pronta a dare una mano

"Risorse umane, Andrea Calhoun."
"Ciao, Andrea, sono Alex della sorveglianza."
"Sì?"
"Come va oggi?"
"Bene. Posso esserti utile?"
"Senti, stiamo preparando un seminario sulla sicurezza per i nuovi assunti e abbiamo bisogno di rintracciare della gente. Mi servono i nomi e numeri di telefono di tutti i nuovi assunti del mese scorso. Puoi aiutarmi?"
"Non ce la faccio prima di oggi pomeriggio. Può andare? Qual è il tuo interno?"
"Va benissimo. 52... ah, però sarò in riunione tutt'oggi. Ti chiamo quando rientro in ufficio, diciamo dopo le quattro."
Quando Alex chiama alle quattro e mezzo, Andrea ha l'elenco pronto, nomi e numeri d'interno.

Un messaggio per Rosemary

Rosemary Morgan è soddisfatta del suo nuovo lavoro. Non ha mai lavorato per una rivista ma trova che i colleghi siano più cordiali del previsto, una lieta sorpresa vista la pressione continua per chiudere il numero per la scadenza mensile. La chiamata che riceve un giovedì mattina non fa che riconfermare questa impressione di cordialità
"Rosemary Morgan?"
"Sì."

"Ciao, Rosemary. Sono Bill Jorday, della sicurezza informazioni."

"Sì?"

"Qualcuno del tuo ufficio ti ha mai spiegato le procedure di sicurezza?"

"Non mi pare."

"Bene, vediamo. Tanto per cominciare non permettiamo a nessuno di installare programmi arrivati da fuori. Questo perché non vogliamo responsabilità per programmi privi di licenza, e anche per evitare problemi di virus."

"Certo."

"Sai della politica per le e-mail?"

"No."

"Qual è il tuo indirizzo?"

"Rosemary@ttrzine.net."

"L'username è Rosemary?"

"R_Morgan."

"Bene. Vorremmo far capire a tutti i nuovi dipendenti che può essere pericoloso aprire un allegato che non aspettano. Arrivano un sacco di virus con le e-mail di gente che non conosci. Perciò se arriva una e-mail non richiesta devi sempre controllare per essere sicura che la persona indicata come mittente ti abbia davvero inviato quel messaggio. Capito?"

"Sì, ne ho sentito parlare."

"Bene, e siamo soliti cambiare la password ogni tre mesi. Tu quando l'hai cambiata?"

"Sono qui da appena tre settimane e sto ancora usando la prima."

"Va bene, puoi aspettare che scadano i novanta giorni. Però dobbiamo essere sicuri che il personale non usi password facili da indovinare. Tu ne hai una di lettere e numeri?"

"No."

"Dobbiamo prowedere. Quale usi?"

"Annette, il nome di mia figlia."

"Non è abbastanza sicura. Non usare mai password con i nomi dei familiari. Vediamo... potresti fare come me. Va bene usare l'attuale come prima parte della password, però ogni volta che la cambi aggiungi il numero del mese corrente."

"Quindi, se lo faccio adesso che è marzo, sarà **3** o **03.**"

"Vedi tu. Come credi meglio."

"Facciamo Annette3."

"Bene. Vuoi che ti spieghi come si fa a cambiare?"

"No, lo so."

"Bene. C'è un'ultima cosa. Tu hai un **antivirus** nel computer ed è importante tenerlo aggiornato. Non devi mai disattivare

l'aggiornamento automatico anche se ogni tanto il computer rallenta. Va bene?"

"Certo."

"Perfetto. E hai il nostro numero per chiamarci se ci sono problemi con il computer?"

Non ce l'ha. Lui le dà il numero, lei lo trascrive con attenzione e poi torna all'opera, contenta di essere seguita tanto premurosamente.

Analizziamo l'attacco

Questo aneddoto batte su un tema che ritroverete lungo tutto il libro: l'informazione più classica che un ingegnere sociale vuole da un dipendente, a parte la preda finale, sono le credenziali di autenticazione della vittima. Con in mano username e password di un singolo dipendente dell'area giusta della ditta, l'attaccante ha tutto quel che gli serve per entrare e localizzare le informazioni che sta cercando. È come avere le chiavi del regno, con quelle in mano può muoversi liberamente nel panorama aziendale per trovare il tesoro.

Prima che i nuovi assunti possano accedere ai sistemi informatici deli'azienda, devono essere preparati a seguire le corrette procedure di sicurezza, soprattutto la pratica di non rivelare mai la propria password.

"L'azienda che non si sforza di proteggere le sue informazioni delicate è negligente e basta." Molti di voi sarebbero d'accordo con un'affermazione del genere e il mondo sarebbe un posto migliore se fosse tutto tanto owio e semplice. In realtà persino le imprese che si sforzano di proteggere le informazioni riservate possono essere in grave pericolo.

Ecco una storia che dimostra per l'ennesima volta come le aziende si ingannino ogni giorno ritenendo che le loro misure di sicurezza, progettate da persone esperte, competenti e professionali, non possano essere aggirate.

La versione di Steve Cramer

Non era un grosso prato, non era uno di quelli dalle sementi pregiate. Non suscitava invidia. E di sicuro non era abbastanza grande da indurlo a comprare un tagliaerbe costoso, che tanto

non avrebbe mai usato. A Steve piaceva falciare il prato con il tagliaerbe a mano perché ci metteva di più e così aveva una scusa valida per starsene per conto suo, invece di ascoltare Anna che gli parlava dei colleghi alla banca in cui lavorava oppure gli spiegava il prossimo lavoretto. Odiava quelle incombenze che erano diventate parte integrante dei suoi fine settimana. Pete, pur avendo appena 12 anni, era stato abbastanza furbo da farsi selezionare nella squadra di nuoto, in modo tale da andare all'allenamento o a una gara e non restare impantanato nei lavoretti del sabato.

Per alcuni il lavoro di Steve, la progettazione di nuovi strumenti sanitari per la GeminiMed Medica1 Products, era una roba noiosa, ma Steve sapeva che salvava delle vite. Si considerava un creativo. Artisti, musicisti, compositori, ingegneri, secondo lui tutti quanti affrontavano la sua medesima sfida, creare qualcosa che nessuno aveva mai fatto prima. E il suo ultimo successo, una protesi cardiaca innovativa, sarebbe stato il più luminoso.

Erano quasi le undici e mezzo di quel sabato, ed era scocciato perché aveva quasi finito di tagliare l'erba senza aver ancora capito come ridurre le esigenze energetiche della protesi, l'ultimo ostacolo rimasto. Un perfetto problema da rimuginare mentre falciava, ma purtroppo non era ancora arrivata la soluzione.

Anna spuntò sulla porta, i capelli coperti dal fazzoletto stile cowboy che indossava sempre quando spolverava. "Telefono. Qualcuno dell'ufficio," gridò.

"Chi?" rispose Steve.

"Ralph Nonsochi, mi pare."

Ralph? Steve non ricordava nessun Ralph alla GeminiMed che potesse chiamarlo a casa, però forse Anna s'era sbagliata.

"Steve, sono Ramon Perez dell'assistenza tecnica." Ramon. Come aveva fatto Anna a trasformare in Ralph un nome classicamente latino? "E solo una telefonata di cortesia," stava intanto dicendo Ramon. "Sono saltati tre server e crediamo sia un worm e adesso dobbiamo cancellare i drive e ripristinare l'ultimo back-up. Possiamo rimettere in funzione i tuoi file per mercoledì o giovedì. Se va bene."

"Assolutamente impossibile," replicò brusco Steve, cercando di non far trasparire la frustrazione. Come facevano a essere tanto stupidi? Credevano sul serio che potesse lavorare senza accedere ai suoi file tutto il weekend e parte della settimana prossima? "Impossibile. Tra un paio d'ore mi piazzo davanti al terminale di casa mia e mi servono i file. È chiaro?"

"Be', tutti quelli che ho chiamato finora vogliono finire in ci-

ma alla lista. Ho rinunciato al fine settimana per venire a risolvere il problema e non è bello che siano tutti incazzati con me."

"Sono sotto pressione, l'azienda conta su di me. Devo finire il lavoro entro oggi pomeriggio. Cos'è che non capisci?"

"Ho ancora da chiamare un sacco di gente prima di mettermi al lavoro. Che ne dici se hai i file per martedì?" propose Ramon.

"No. Non martedì o lunedì, ADESSO!" esclamò Steve, chiedendosi a chi poteva rivolgersi se non riusciva a fare entrare il concetto nella testaccia di quel demente.

"Va bene, va bene." Ramon fece un sospiro scocciato. "Vediamo cosa posso fare per te. Tu usi il server RM22, vero?"

"RM22 e GM16. Entrambi."

"Giusto. Bene, posso risparmiare un po' di tempo. Però mi servono username e password."

Oh-oh, che succede? Perché? Proprio uno della IT? pensa Steve.

"Come hai detto che fai di cognome? E chi è il tuo superiore?"

"Ramon Perez. Ti dico una cosa. Quando ti hanno assunto ti hanno dato un modulo da compilare per avere l'account utente, e hai deciso una password. Posso darci un'occhiata per controllare cos'abbiamo registrato qui. Ti va bene?"

Steve rifletté per qualche secondo, poi accettò. Attese con crescente impazienza, mentre Ramon andava a recuperare il modulo in uno schedario. Alla fine lo sentì sfogliare una pila di scartoffie.

"Eccolo. Hai messo come password 'Janice'," disse alla fine Ramon.

Janice. Era il nome di sua madre che usava ogni tanto come password. In effetti poteva avere scelto quello quando aveva compilato i moduli d'assunzione.

"Esatto," ammise.

"Stiamo solo perdendo tempo. Adesso hai capito che non sono un impostore, e se vuoi riavere i tuoi file al volo devi darmi una mano."

"La mia ID è sd-lineetta bassa-cramer. La password è 'pelican1'."

"Mi ci metto subito, dammi un paio d'ore," concluse Ramon, di nuovo conciliante.

Steve finì il prato, mangiò e tornato al computer scoprì che i suoi file c'erano tutti. Era soddisfatto di avere ammorbidito in maniera tanto volitiva quell'antipatico della IT, e sperava che Anna l'avesse sentito. Sarebbe stato il caso di congratularsi con il tipo o con il suo capo, ma era una di quelle cose che sapeva non avrebbe mai fatto.

La versione di Craig Cogburne

Craig Cogburne aveva lavorato come rappresentante in una ditta di hi-tech, ed era anche bravo. Dopo un po' s'era accorto di essere in gamba a interpretare il cliente, a capire dove faceva resistenza e riconoscere le debolezze che potevano facilitare la chiusura della vendita. Cominciò quindi a pensare ad altri modi per sfruttare quel talento, approdando al campo più ricco: lo spionaggio industriale.

Questo era un incarico delicato. Non sembrava molto lungo e valeva abbastanza da finanziare un viaggetto alle Hawaii. O forse a Tahiti.

Il tipo che mi aveva assunto non mi aveva detto chi era il cliente, owio, però sembrava un'azienda che voleva mettersi in pari con la concorrenza con un disinvolto passo da gigante. Dovevo solo ottenere i progetti di un nuovo oggettino, una protesi cardiaca, di qualunque cosa si trattasse. La ditta si chiamava GeminiMed. Mai sentita, però era una roba da prime cinquecento nella lista di "Fortune" con sedi in una decina di posti, il che rende il lavoro più facile perché ci sono meno possibilità che il tipo con cui parli conosca la persona che fingi di essere e ti scopra. E questo, come dicono i piloti a proposito delle collisioni in volo, è sufficiente a rovinare una bella giornata.

Il mio cliente mi mandò un fax con una pagina di una rivista medica che annunciava che la GeminiMed stava lavorando su una protesi dal concetto rivoluzionario, che si sarebbe chiamata STH-100. Ammettiamolo, quel giornalista aveva già fatto un bel po' di ricerche sul campo al posto mio. Già prima di partire avevo una cosa che mi serviva, il nome del nuovo prodotto.

Primo problema: ottenere i nomi dei dipendenti che lavoravano sull'STH-100 o potevano vedere i prototipi. Così chiamai il centralino dicendo: "Ho promesso a uno del gruppo progettazione che mi sarei fatto vivo ma non ricordo come si chiama. Però so che di nome comincia con S".

La donna rispose: "Abbiamo uno Scott Archer e un Sam Davidson".

Io rischiai. "Chi è quello che lavora nel gruppo STH-100?" Lei non lo sapeva, perciò provai con Scott Archer, che la centralinista mi passò direttamente.

Quando Scott rispose gli dissi: "Ciao, sono Mike, della stanza della posta. Abbiamo un pacco per corriere per la squadra del progetto STH-100. Hai idea a chi deve andare?". Scott mi diede il nome del direttore del progetto, Jerry Mendel. Riuscii persino a convincerlo a darmi il suo numero.

Telefonai. Mendel era fuori ma la segreteria telefonica spiegò

che era in vacanza fino al **13,** il che significava che aveva ancora una settimana da sciare o quel che era, comunque se si aveva bisogno si poteva sentire Michelle al **9137.** Molto gentili, quelli. Dawero molto gentili.

Appesi e chiamai Michelle. "Sono Bill Thomas. Jerry mi ha detto di chiamarti appena avevo pronte le specifiche da far controllare ai ragazzi della sua squadra. State lavorando sulla protesi cardiaca, vero?" Michelle rispose di sì.

Adesso si arrivava alla parte spinosa. Se per caso l'amica si insospettiva ero pronto a giocare la carta "sto solo facendo un favore chiestomi da Jerry". "In che sistema sei?"

"Sistema?"

"Che server usa il tuo gruppo?"

"Oh. **RM22.** Alcuni anche GM**16.**"

Perfetto. Mi serviva, ed era **un'informazione** che le avevo strappato senza insospettirla. E che la rese **più** malleabile per il prossimo pezzo, da me recitato con la massima disinvoltura. "Jerry ha detto che potevi darmi una lista di indirizzi di posta elettronica di quelli del gruppo di sviluppo," dissi, trattenendo il fiato.

"Certo. La lista di distribuzione è troppo lunga, ma posso farti una e-mail."

Ops. Qualsiasi indirizzo che non finiva con GeminiMed.com avrebbe fatto scattare il campanello d'allarme. "Perché non me la faxi?"

Nessun problema.

"Il nostro apparecchio è guasto ma posso farmi dare il numero di un altro. Ti richiamo," dissi prima di appendere.

Penserete che adesso ero nelle peste, ma è solo un banale trucco del mestiere. Attesi un attimo perché la voce non suonasse familiare alla centralinista, poi la richiamai. "Salve, sono Bill Thomas. **Il** nostro fax non funziona. Posso farlo arrivare da voi?" Lei disse di sì e mi diede il numero.

Allora sono passato a prenderlo, giusto? Sbagliato. Prima regola: mai andare di persona sul posto a meno che non sia assolutamente necessario. È dura identificarti finché rimani solo una voce al telefono. Ma appena ti identificano ti arrestano. Invece non si ammanetta una voce. Quindi richiamai dopo un po' la centralinista per chiederle se era arrivato il fax, e lei rispose di sì.

Le dissi: "Senta, devo mandarlo a un consulente. Può spedirglielo lei per me?" Certo. E perché no, come fa una centralinista a riconoscere i dati scottanti? Mentre lei spediva i dati al "consulente" io feci un po' di ginnastica andando in una cartoleria provvista del cartello "Fax". Il mio doveva essere già arrivato, e in effetti mi stava aspettando quando entrai. Sei pagine per un

dollaro e 75. Per un deca e spiccioli avevo l'intera lista di nomi con gli indirizzi di posta elettronica.

Entrare

Bene, adesso avevo parlato con tre o quattro persone diverse in poche ore ed ero molto più vicino ai computer dell'azienda. Però prima di cantare vittoria avevo bisogno di un altro paio di dettagli.

Il primo era il numero di telefono per chiamare il server della progettazione dall'esterno. Richiamai la GeminiMed chiedendo alla centralinista il settore IT, e al tizio che rispose domandai se c'era qualcuno che poteva aiutarmi con il computer. Quando me lo passò, finsi di essere confuso e un po' ignorante di questioni tecniche. "Sono a casa, ho appena comprato un portatile e devo settarlo per chiamare dall'esterno."

La procedura era banale ma lasciai che lui mi accompagnasse passo passo fino al numero che mi comunicò come se fosse un'informazione banale. Poi lo feci aspettare mentre provavo. Perfetto.

Avevo superato l'ostacolo della connessione alla Rete. Quando feci il numero vidi che avevano un server che permetteva a chi chiamava di collegarsi a ogni computer della rete interna. Dopo una serie di tentativi incontrai una macchina dove potevi registarti come ospite, senza bisogno di password. Alcuni sistemi operativi, quando vengono installati, richiedono ID e password, ma forniscono anche un guest account. L'utente dovrebbe impostare la propria password anche in questo account oppure disattivarlo, ma molta gente non lo sa o non si preoccupa. Quel sistema era stato appena installato e il suo proprietario non s'era crucciato a disabilitare il guest account.

Grazie a lui, adesso potevo entrare in un computer con una vecchia versione di UNIX. In UNIX il sistema operativo conserva un file che contiene le password crittate di tutti coloro che sono autorizzati a quella macchina, cioè ha l'hash univoco (una codificazione irreversibile) delle password di ogni utente. Con un hash univoco una password apparirà in forma crittata, convertita da UNIX in caratteri alfanumerici.

Quando Billy Bob dell'ufficio accanto vuole trasferire dei file a un computer, deve identificarsi con username e password, e il programma di sistema che controlla la sua autorizzazione codifica la password che viene inserita e la confronta con l'hash contenuto nel file password. Se combaciano autorizza l'accesso.

Essendo le password cifrate, il file era accessibile a ogni utente dato che ritenevano impossibile decifrarle. Che ridere. Scari-

cai il file, lo passai al vocabolario (vedi il capitolo **12** per altre notizie su questo metodo) e trovai che un progettista, un tale Steven Cramer, aveva un account su quel computer con la password "Janice". Già che c'ero, tentai di usare la sua password su un server dello sviluppo. Se avesse funzionato mi avrebbe risparmiato tempo e qualche rischio. Non funzionò.

Significava che avrei dovuto convincere il tipo a dirmi username e password. Per questo dovevo aspettare il fine settimana.

Sapete già il resto. Al sabato chiamai Cramer rifilandogli, per non insospettirlo, una storia su un worm e sui server che dovevano essere ripristinati con l'ultimo back-up.

E la storia che gli raccontai, quella della password che aveva dato quando aveva riempito i moduli di assunzione? Contavo sul fatto che non si ricordasse. Un nuovo dipendente riempie tante scartoffie che anni dopo chi se ne ricorda più? E comunque, anche se avessi toppato con lui, avevo un lungo elenco di nomi alternativi.

Entrai nel server con username e password di Cramer, cercai per un po' in giro e poi localizzai i file progettazione dell'STH-**100.** Non ero del tutto sicuro di quali potessero essere quelli cruciali, perciò trasferii tutti i file in una dead drop, un sito FTP gratis in Cina dove potevo conservarli senza suscitare sospetti. Che ci pensasse il cliente a smazzare il mucchio per scovare quel che voleva.

Analizziamo l'attacco

Per il nostro Craig Cogburne, o quelli come lui abili nelle arti furtive-ma-non-sempre-illegali dell'ingegneria sociale, la sfida qui presentata era quasi banale. Doveva localizzare e impossessarsi dei file conservati in un computer aziendale sicuro protetto da un firewall e da tutte le solite tecnologie di sicurezza.

Nel complesso s'è trattato di una passeggiata. Ha iniziato facendosi passare per un addetto alla distribuzione della posta aggiungendo una certa nota d'urgenza con la faccenda del pacchetto da consegnare. Questo trucco ha sortito il nome del capo della squadra del gruppo di progettazione della protesi, che era in vacanza ma (comodissimo per l'ingegnere sociale che vuol rubare informazioni) aveva gentilmente lasciato il nome e numero di telefono della sua assistente. Quando ha chiamato la donna, Craig ha sventato i sospetti sostenendo che stava agendo su richiesta del capo. Visto che questi era fuori città, Michelle non poteva verificare se era dawero così e quindi ha pensato che fosse vero e ha fornito senza problemi un elenco di componenti

della squadra, un'informazione necessaria e di assoluto valore per Craig.

Non si è insospettita nemmeno quando Craig ha chiesto di farsi mandare l'elenco per fax invece che per posta elettronica, di solito molto più comoda per entrambi. Perché è stata tanto sventata? Come tanti dipendenti, non voleva che il capo al suo ritorno scoprisse che aveva scoraggiato una persona che voleva solo fare quello che gli era stato richiesto. E poi quell'uomo aveva detto che il capo non aveva soltanto autorizzato la richiesta ma aveva domandato il suo aiuto. Ancora un esempio di persona che dimostra una gran voglia di far parte di una squadra, un desiderio che rende tanti di noi vulnerabili agli inganni.

Craig ha evitato il rischio di entrare di persona nell'edificio facendosi inviare il fax dalla centralinista, intuendo che era una ragazza disponibile. In fondo, di solito le centraliniste e le segretarie sono scelte per la loro gentilezza e la capacità di suscitare una buona impressione. Un piccolo favore come reindirizzare un fax fa parte del lavoro, un dettaglio di cui Craig si è approfittato. C'è da dire che il tipo di informazione che la giovane ha inviato doveva far scattare l'allarme, essendo al corrente del suo valore. Ma come pretendere che una come lei sapesse distinguere le informazioni innocue da quelle delicate?

Passando a una manipolazione diversa, Craig è parso confuso e ingenuo per convincere il tipo dell'IT a fornirgli il numero di accesso al terminal server, la macchina che funge da collegamento con gli altri sistemi informatici della rete interna.

Craig è riuscito a collegarsi facilmente provando una password di default mai cambiata, uno di quei buchi clamorosi che rimangono in tante reti interne, la cui sicurezza si basa sui firewall. Anzi, le password di default di tanti sistemi operativi, router e simili, compresi i PBX, sono reperibili in Rete. Qualsiasi ingegnere sociale, hacker o spia industriale, e anche un semplice curioso, può trovare la lista in http://www.phenoelit.de/dpl/dpl.html. (È incredibile quanto Internet faciliti l'esistenza a chi sa dove andare a guardare. Adesso lo sapete anche ***voi.)***

> La priorità di chiunque in un'impresa è completare il proprio lavoro in tempo. Quando si è sottoposti a questa pressione spesso le procedure di sicurezza passano in secondo piano e sono trascurate o ignorate. Gli ingegneri sociali si basano su questo dato di fatto quando mettono in pratica le loro risorse.

Poi Cogburne è riuscito a convincere un tipo cauto e sospettoso ("Come ha detto che si chiama? Chi è il suo superiore?") a dargli username e password per accedere ai server usati dalla sua squadra. Era come lasciargli la porta aperta per ficca-

nasare nei segreti più sorvegliati dell'azienda e scaricare i progetti del nuovo prodotto.

E se Steve Cramer fosse rimasto sulle sue? Era comunque improbabile che segnalasse i suoi sospetti fino al ritorno in ufficio il lunedì mattina, quando ormai sarebbe stato troppo tardi.

Una chiave per l'ultima parte del raggiro: all'inizio Craig è sembrato poco interessato ai problemi di Steve, poi ha cambiato registro e l'ha fatto sembrare come se lo stesse aiutando a completare il suo lavoro. Se la vittima si convince che la stai aiutando o che le stai facendo un favore, quasi sempre rivelerà informazioni riservate che altrimenti avrebbe protetto con attenzione.

PREVENIAMO GLI ATTACCHI

Uno dei trucchi più efficaci dell'ingegneria sociale è quello di "rigirare la frittata", come avete visto in questo capitolo. L'ingegnere sociale crea il problema e poi lo risolve magicamente, convincendo la vittima a fornirgli l'accesso ai segreti più protetti dell'azienda. I vostri dipendenti possono cascarci? Vi siete dati la pena di stilare e diffondere specifiche regole di sicurezza che possano impedirlo?

Educare, educare, e ancora educare...

C'è una vecchia barzelletta su un turista che a New York ferma un tale per strada per chiedergli come si fa ad arrivare alla Carnegie Hall, la famosa sala concerti. Quello risponde: "Esercitarsi, esercitarsi, esercitarsi". Tutti sono talmente vulnerabili agli attacchi degli ingegneri sociali che l'unica difesa efficace di un'azienda è quella di educare e formare il personale, dandogli l'esperienza necessaria per individuare un ingegnere sociale, ricordando in continuazione ai dipendenti ciò che hanno appreso.

Tutti quanti devono essere addestrati a mostrare un certo livello di sospettosità e cautela quando sono contattati da chi non conoscono di persona, soprattutto allorché costui chiede accesso a un computer o a una rete. Fa parte della natura umana fidarsi degli altri, però, come dicono i giapponesi, gli affari sono una guerra. I vostri affari non possono permettersi di abbassare la guardia. La politica di sicurezza dell'azienda deve specificare chiaramente i comportamenti adatti e quelli inadatti.

La sicurezza non ha una taglia unica. Di solito, il personale ri-

copre ruoli e responsabilità diversi e ogni posizione ha una determinata vulnerabilità. Dovreste garantire un livello base di preparazione a tutti, dopodiché il personale deve essere addestrato anche secondo i rispettivi incarichi a scoprire certe procedure che possano ridurre la possibilità che i singoli dipendenti diventino parte del problema. Quanti lavorano con informazioni sensibili o ricoprono una posizione di fiducia dovrebbero passare attraverso un ulteriore addestramento specializzato.

Tenere al sicuro le informazioni delicate

Quando una persona viene accostata da un estraneo che si offre di aiutarla, come abbiamo visto in questo capitolo, deve ricorrere alla politica di sicurezza aziendale adattata alle necessità, dimensioni e cultura della vostra azienda.

Mai collaborare con un estraneo che vi chiede di cercare un'informazione, di dare comandi insoliti a un computer, di cambiare le impostazioni del software oppure, la cosa potenzialmente più disastrosa, di aprire un allegato di e-mail o scaricare software non controllato. Qualsiasi programma, persino quello che non sembra fare alcunché, potrebbe non essere innocente come sembra.

Ci sono certe procedure che tendiamo nel tempo a trascurare, per quanto possa essere stato valido l'addestramento. Poi ce ne scordiamo completamente proprio quando verrebbe utile. Mi direte che lo sanno tutti (o dovrebbero sapere tutti) che non bisogna mai dare la user ID o la password, non dovrebbe nemmeno essere ripetuto: è banale buon senso. Ma nella realtà bisogna rammentare spesso a ogni dipendente che rivelare username o password del computer in ufficio o a casa o persino della macchina di affrancatura della posta aziendale equivale a dare il PIN del Bancomat.

Capitano ogni tanto (anzi, spesso) circostanze in cui è necessario, forse addirittura importante, rivelare a terzi un'informazione riservata. Perciò non è sensato fare del "mai" una regola assoluta. Tuttavia, le vostre procedure di sicurezza devono essere molto specifiche sulle circostanze in cui un dipendente è autorizzato a svelare la sua password e, soprattutto, su chi è autorizzato a chiedere una simile informazione.

Valutare la fonte

In molte organizzazioni la regola invalsa dovrebbe essere che ogni informazione che può danneggiare la ditta o un collega de-

ve essere rilasciata soltanto a chi è noto di persona, o la cui voce è tanto familiare da essere riconosciuta senza equivoci.

Nelle situazioni che necessitano un elevato livello di sicurezza le uniche richieste da esaudire sono quelle consegnate di persona o con un suggello forte, per esempio due elementi separati come un segreto condiviso e un token temporizzato.

Le procedure di riservatezza dei dati devono specificare chiaramente che *nessuna* informazione possa uscire da un settore coinvolto in lavori chiave a favore di individui che non sono conosciuti di persona o che non sono garantiti in qualche modo.

Allora come gestire una richiesta che sembra legittima da parte di un collega, come un elenco di nomi e di indirizzi di posta elettronica del vostro gruppo? Come rendere consapevoli del fatto che un dato del genere, chiaramente meno prezioso delle specifiche di un prodotto in via di sviluppo, debba essere considerato di esclusivo utilizzo interno? Una gran parte della soluzione sta nell'indicare i dipendenti di ogni settore che gestiranno tutte le richieste di informazioni da far trapelare dal gruppo. Quindi fornire un programma avanzato di preparazione alla sicurezza per far comprendere ai dipendenti designati le speciali procedure di verifica che devono rispettare.

Non dimenticare nessuno

Chiunque è in grado di snocciolare in fretta le strutture nella propria ditta che hanno bisogno di un alto livello di protezione contro attacchi di malintenzionati, però spesso trascuriamo altri posti meno owi eppure assai vulnerabili. In una di queste storie la richiesta di inviare un fax a un numero di telefono entro la ditta sembrava abbastanza innocente, eppure l'attaccante si è approfittato di questa falla nella sicurezza. Qual è la lezione da trarre? Tutti, dalle segretarie ai dirigenti, devono superare uno speciale training per diventare consapevoli di questo genere di trucchi. E non dimenticate di sorvegliare il portone d'ingresso: anche gli addetti all'accoglienza diventano spesso i primi bersagli degli ingegneri sociali e devono capire le tecniche subdole che possono usare i visitatori e le persone che telefonano.

La sicurezza aziendale dovrebbe definire un singolo posto di contatto, una specie di punto di smistamento per i dipendenti convinti di essere stati vittime di un raggiro. Un singolo posto a cui riferire questi incidenti di sicurezza garantisce un efficace sistema di allarme tempestivo che farà capire al volo quando è in corso un attacco, in modo che i danni possano essere controllati immediatamente.

6.
"Può aiutarmi?"

Avete visto come gli ingegneri sociali riescano a ingannare la gente offrendole aiuto. Un'altra tattica classica sceglie la procedura inversa: l'ingegnere sociale manovra la vittima fingendo di avere bisogno che l'altro gli dia una mano. Tutti noi simpatizziamo per le persone nei guai, perciò spesso questa tattica si dimostra efficace per aiutare l'ingegnere sociale a raggiungere il suo scopo.

Una storia del terzo capitolo vi ha dimostrato come l'attaccante riesce a convincere la vittima a rivelargli il suo Ssn (il numero di Sicurezza sociale). La prossima userà una strategia diversa per arrivare al medesimo risultato, dopodiché l'attaccante potrà sfruttare l'informazione ottenuta.

Stare al passo con i Jones

A Silicon Valley c'è una certa azienda globale che lasceremo innominata. Gli uffici vendite e i vari stabilimenti sparsi nel pianeta sono tutti collegati alla sede centrale tramite una "wide area network", WAN. L'intruso, un tipo sveglio e petulante che chiamaremo Brian Atterby, sapeva che è quasi sempre più facile entrare in una rete da un sito remoto, dove la sorveglianza è sicuramente più distratta che nella sede centrale.

Ha telefonato all'ufficio di Chicago chiedendo del signor Jones. Quando la segretaria ha chiesto se sapeva come faceva di

nome lui ha risposto: "Lo sto cercando. Perché, quanti Jones avete?".

"Tre. In quale ufficio lavora?"

"Se mi dice i nomi forse lo riconosco."

"Barry, Joseph e Gordon."

"Joe. Ne sono pressoché sicuro. Ed era... in quale ufficio?"

"Sviluppo affari."

"Certo. Può passarmelo, per favore?"

Lei glielo passa. Quando Jones risponde l'attaccante dice: "Signor Jones? Salve, sono Tony dell'ufficio paghe. Abbiamo appena accettato la sua richiesta di depositare direttamente la busta paga sul suo conto corrente alla Credit Union."

"COSA???!!!Starà scherzando. Non ho mai fatto una richiesta del genere. Non ho nemmeno un conto alla Credit Union."

"Accidenti, l'ho appena mandata."

Jones è a dir poco imbufalito che il suo stipendio finisca nel conto di un altro, e sta cominciando a temere che il tizio all'altro capo del filo sia un tantino tardo di comprendonio. Prima che possa dire altro, l'attaccante aggiunge: "È meglio se controllo. I cambiamenti nelle buste paga sono accompagnati dal numero del dipendente. Qual è il suo?"

Jones glielo dà. Allora l'altro aggiunge: "No, ha ragione, non era una sua richiesta".

Jones pensa che diventano sempre più stupidi ogni anno che passa.

"Senta, vedo di risolvere. Correggo subito. Non si preoccupi, avrà la sua busta paga entro oggi," lo rassicura il sedicente Tony.

Un viaggio di lavoro

Poco dopo l'amministratore di sistema dell'ufficio vendite di Austin, nel Texas, riceve una telefonata. "Sono Joseph Jones, dello sviluppo affari nella sede centrale. Sarò in città questa settimana, al Driskill Hotel. Vorrei che mi aprisse un account temporaneo per poter accedere alla posta senza fare un'interurbana," spiega chi chiama.

"Mi ripete il nome, e mi dà il numero di matricola?" chiese l'amministratore. Il falso Jones obbedisce aggiungendo: "Avete numeri di accesso su linea commutata ad alta velocità?".

"Rimanga in linea, la verifico sul database." Dopo un po': "A posto, Joe. Mi dica, qual è il numero del suo edificio?". Visto che l'attaccante ha fatto i compiti a casa ha la risposta pronta.

"Perfetto, mi ha convinto," dice l'amministratore di sistema.

Semplice semplice. Ha verificato il nome Joseph Jones, l'ufficio e il numero di matricola, e alla fine "Joe" gli ha dato la ri-

> Non basatevi sui firewall e le protezioni di Rete per tutelare le vostre informazioni. Cercate sempre i punti deboli, che di solito sono le persone.

sposta giusta alla domanda di conferma. "Come username avrà quello aziendale, jbjones, e la password iniziale è 'changeme'," conclude.

Analizziamo l'attacco

Con un paio di telefonate e quindici minuti di tempo l'attaccante ha ottenuto l'accesso alla wide area network dell'azienda, che come tante possiede quella che chiamo una "sicurezza caramella" (candy security), secondo la definizione di due ricercatori dei Bell Labs, Steve Bellovin e Steven Cheswick, che descrivono una sicurezza del genere come "un guscio croccante con un cuore morbido", un po' come le noccioline M&M's. Il guscio esterno, il firewall, secondo Bellovin e Cheswick, non è una protezione sufficiente perché se l'intruso riesce ad aggirarlo i sistemi informatici interni forniscono una sicurezza molle. Quasi sempre non sono adeguatamente protetti.

Questa storia calza a pennello con una simile definizione. Con un numero di modem e un account l'attaccante non deve nemmeno preoccuparsi di sconfiggere un firewall Internet, e una volta dentro può tranquillamente manomettere quasi tutti i sistemi della rete interna.

A quanto mi risulta proprio questo trucco è stato usato contro uno dei più grossi produttori di software al mondo. Verrebbe da pensare che gli amministratori di sistema in un'azienda del genere siano preparati a individuare questo genere di truffe, ma in base alla mia esperienza so che nessuno può ritenersi completamente al sicuro se un ingegnere sociale è furbo e abbastanza convincente.

SICUREZZA IN STILE SPEAKEASY

Ai tempi degli speakeasy, quei localini dell'era del Proibizionismo dove scorrevano fiumi di gin, un candidato avventore poteva essere ammesso solo andando a bussare alla porta. Dopo qualche secondo si apriva uno spioncino al quale si affacciava un volto duro e intimidente. Se il visitatore era uno del giro citava un cliente fisso del posto (spesso bastava un "mi manda Joe"), e a quel punto il buttafuori apriva la porta e lo faceva entrare.

Il vero trucco consisteva nel conoscere dove si trovava lo

speakeasy perché non c'erano insegne e il proprietario non era certo interessato a installare un neon per segnalare la sua presenza. Di solito, essere arrivato nel posto giusto era più che sufficiente per essere anche autorizzato all'accesso. Purtroppo lo stesso livello di salvaguardia è comunemente praticato nel mondo delle imprese, garantendo una non protezione che io chiamo sicurezza in stile speakeasy.

*L'ho **visto** al **cinema***

Ecco un esempio tratto da un classico che molti ricorderanno. Ne *I* tre giorni del Condor il protagonista Turner, impersonato da Robert Redford, lavora per una piccola struttura di ricerca sotto contratto con la CIA. Un giorno, quando rientra dalla pausa pranzo, scopre che i suoi colleghi sono stati ammazzati a pistolettate e deve capire chi è stato e perché, sapendo tra l'altro che i cattivi, chiunque essi siano, lo stanno cercando per eliminarlo.

A un certo punto Turner riesce a ottenere il numero di telefono di un cattivo. Ma chi è, e come fa Turner a localizzarlo? Ha fortuna: lo sceneggiatore David Rayfiel gli ha simpaticamente regalato un passato nel Genio radiotelegrafisti, e quindi il protagonista del film conosce tecniche e usanze delle compagnie telefoniche. Avendo il numero del cattivo, adesso sa come procedere. Nel copione la scena è la seguente:

Turner si ricollega e compone un altro numero. Drin! Drin! Poi:

Voce di donna (*filtrata*)
CNA, signora Coleman.

Turner (nel set collaudo)
Sono Harold Thomas, signora Coleman. Servizio clienti. CNA per 202-555-7389, per favore.

Voce di donna (*filtrata*)
Un momento, prego.
(e quasi immediatamente)
Leonard Atwood, 765 MacKensie Lane, Chevy Chase, Maryland.

Tralasciando il piccolo dettaglio che lo sceneggiatore usa per sbaglio un prefisso di Washington per un indirizzo del Maryland, avete capito cos'è successo?

Il concetto di "security through obscurity" non ha la *minima* efficacia nel bloccare gli attacchi. Ogni sistema informatico al mondo ha almeno un essere umano che lo utilizza. Se l'attaccante è in grado di ingannare la gente che usa i sistemi, l'oscurità del sistema diventa ininfluente.

Turner, grazie al training come cablatore telefonico, sapeva quale numero doveva comporre per raggiungere l'ufficio dell'azienda telefonica chiamato CNA, il servizio nomi e indirizzi clienti per gli installatori e altro personale autorizzato. L'impiegata del CNA ha risposto dandogli il nome e indirizzo della persona a cui apparteneva quel numero.

Ingannare l'azienda telefonica

Nel mondo reale il numero del CNA è un segreto gelosamente custodito. Anche se le compagnie telefoniche si sono adeguate e oggi sono meno generose con le informazioni, in quegli anni applicavano una variante della sicurezza in stile speakeasy che i professionisti del ramo chiamano "sicurezza tramite oscurità" (security through obscurity). Presumevano insomma che tutti quelli che chiamavano il CNA e conoscevano il gergo adatto (per esempio, "servizio clienti, CNA per 555-1234, per favore") fossero persone autorizzate.

Non c'era alcun bisogno di verificare o identificarsi, di dare un riferimento di matricola, una password che cambiava tutti i giorni. Se sapevi quale numero chiamare e sembravi genuino, allora avevi diritto all'informazione.

Non era un assunto molto solido da parte dell'azienda telefonica. L'unico sforzo che facevano era cambiare periodicamente il numero di telefono, almeno una volta all'anno, ma anche così il numero in un dato momento diventava ampiamente noto tra i phreak, che si divertivano a sfruttare questa comoda fonte di dati informando i loro colleghi. L'esistenza dell'ufficio CNA è stata una delle prime cose apprese quando sono entrato nel giro dei phreaker.

In tutto il settore delle imprese e degli enti statali la sicurezza in stile speakeasy è ancora maggioritaria. È assai probabile che un qualsiasi intruso anche parzialmente abile riesca a farsi passare da persona autorizzata soltanto mettendo insieme abbastanza informazioni su settori, persone e gergo della vostra struttura. Certe volte non occorre nemmeno quello: basta un numero di interno.

IL SUPERFICIALE IT MANAGER

Anche se tanti dipendenti di una struttura possono essere negligenti, poco interessati o ignari, dareste per scontato che un manager del centro informatico di una multinazionale conosca per filo e per segno le migliori pratiche di sicurezza. Giusto?

Non vi aspettereste mai che costui, facente parte del settore Information Technology dell'azienda, possa cadere vittima di una banale e ovvia manovra di ingegneria sociale. ***Soprattutto*** se l'ingegnere sociale è poco più di un ragazzo. Però ogni tanto si prevede male.

Sintonizzarsi

Anni fa, un divertente passatempo di tanta gente era di tenere la radio sintonizzata sulle frequenze della polizia o dei pompieri per ascoltare le conversazioni concitate sulle rapine in corso, su un incendio in un palazzo o un inseguimento in macchina nel pieno del loro svolgimento. Le frequenze radio usate dai tutori dell'ordine, persino a livello federale, e dai vigili del fuoco erano reperibili nei volumi in vendita in tutte le librerie, mentre oggi sono elencate sul Web e su un libro distribuito nella catena Radio Shack.

Owiamente, non erano sintonizzati solo i curiosi. I ladri che rubavano in un negozio in piena notte restavano in ascolto per sentire se stavano per caso inviando una volante dalle loro parti. Gli spacciatori controllavano l'attività degli agenti della DEA, i piromani se la ridevano prima appiccando il fuoco e poi ascoltando le conversazioni radio mentre i pompieri cercavano di spegnerlo.

I recenti progressi nella tecnologia informatica hanno reso possibile cifrare le comunicazioni vocali. Adesso che è diventato più semplice infilare una potenza enorme in un solo microchip, sono arrivate le piccole radio cifrate per i poliziotti proprio per impedire che cattivi e curiosi origliassero.

Danny l'intercettatore

Un entusiasta ficcanaso e hacker provetto che chiameremo Danny decide di vedere se trova la maniera di mettere le mani su un supersegreto programma di cifratura, il codice sorgente di uno dei maggiori produttori di sistemi per la sicurezza radiofonica. Spera, studiando il codice, di poter capire come spiare le forze dell'ordine e casomai usare quella tecnologia per impedire alle più potenti agenzie governative di monitorare le sue conversazioni con gli amici.

I Danny del sottobosco hacker appartengono a una categoria speciale che si situa tra i solo-curiosi-e-totalmente-innocuie i tipacci pericolosi. I Danny uniscono le competenze dell'esperto alla maligna pulsione hacker di entrare nei sistemi e nelle reti,

solo per il piacere di farlo e per la sfida intellettuale di vedere dal di dentro come funziona la tecnologia. Però le loro effrazioni elettroniche sono soltanto bravate. Questi hacker buoni entrano illegalmente nei siti per puro divertimento e per dimostrare di saperlo fare. Non rubano niente, non guadagnano un soldo dalle loro imprese, non distruggono file né sabotano connessioni di rete né tantomeno danneggiano sistemi informatici. Il solo fatto che siano lì a fregare copie di file e leggere le e-mail con le password alle spalle della sicurezza e degli amministratori di rete fa prudere le mani di coloro che sono incaricati di tenere alla larga intrusi del genere. Essere sempre un passo avanti agli altri costituisce la maggior parte della soddisfazione.

Facendo onore a questo ritratto, il nostro Danny voleva sbirciare i dettagli del prodotto più protetto della compagnia bersaglio, solo per soddisfare la sua curiosità bruciante e per ammirare le brillanti innovazioni escogitate dal produttore.

Non c'è bisogno di aggiungere che quei piani erano segreti commerciali attentamente sorvegliati, valutati e protetti come i beni più preziosi dell'azienda. Danny lo sapeva. E non gliene fregava niente. In fondo era solo una grossa azienda anonima.

Ma come ottenere il codice sorgente? Si scoprì poi che sgraffignare i gioielli della corona dal Scg (Secure Communications Group) dell'azienda era sin troppo facile, anche se l'impresa era una di quelle che usava la cosiddetta "autenticazione a due fattori", che richiede l'utilizzo non di uno bensì di due identificatori per dimostrare chi sei.

Ecco un esempio che non vi suonerà nuovo. Quando arriva la nuova carta di credito, vi chiedono di telefonare all'istituto di rilascio per fargli sapere che la carta è in possesso del cliente previsto e che non è stata trafugata dalla posta. Attualmente le istruzioni allegate alla carta vi consigliano di solito di chiamare *da casa*. Quando telefonate, un programma dell'istituto di credito analizza l'ANI (Automatic Number Identification), l'identificazione automatica della chiamata fornita dal centralino del numero verde dell'istituto.

Un computer presso l'istituto della carta di credito prende il numero del chiamante fornito dall'ANI e lo confronta con il database dei possessori di carta della compagnia. Quando l'impiegato risponde, il suo schermo gli mostra le informazioni del database con i dati del cliente, perciò sa già che la chiamata arriva dall'abitazione giusta. Questa è una prima forma di autentica.

Poi l'impiegato sceglie una voce tra le informazioni che vi riguardano, di solito il numero di previdenza sociale, la data di nascita o il cognome da ragazza della madre, e vi pone una domanda. Se date la risposta esatta ecco la seconda autentica, basata su informazioni di cui dovreste essere al corrente.

Presso l'azienda che produce i sistemi radio sicuri della nostra storia ogni dipendente con accesso al computer aveva username e password come tutti, ma in più disponeva di un aggeggino elettronico chiamato Secure ID, un cosiddetto "time-based token". Questi strumenti sono di due tipi, uno grande circa come una carta di credito ma un tantino più spesso, l'altro talmente piccolo che molti l'attaccano al portachiavi.

Questo gadget ereditato dal mondo della crittografia ha un piccolo display con una serie di sei numeri che ogni sessanta secondi mostra una cifra diversa. Quando una persona autorizzata vuole accedere alla rete da fuori sede deve prima identificarsi come utente autorizzato battendo il PIN segreto e i numeri evidenziati dallo strumento. Una volta verificati questi dati dal sistema interno, la persona inserirà nome dell'account e password.

Per arrivare all'agognato source code il giovane hacker Danny doveva non solo procurarsi username e password di un dipendente (poca roba per un ingegnere sociale esperto) ma anche risolvere questo problema.

Battere l'autenticazione a due fattori di un token a tempo associato a un PIN segreto suona come una sfida tipo *Missione impossibile,* ma l'ingegnere sociale è come un giocatore di poker molto abile nel leggere gli avversari. Quando si siede al tavolo da gioco sa che con molta probabilità, con una piccola spinta della fortuna, se ne andrà con un bel po' di soldi altrui.

Attaccare la fortezza

Danny iniziò facendo i compiti a casa, e in men che non si dica riuscì a mettere insieme abbastanza elementi da farsi passare per un vero dipendente. Aveva nome, settore, numero di telefono e numero di matricola, oltre al nome e numero d'interno del capoufficio.

Adesso veniva la calma prima della tempesta. In senso letterale. Per il felice esito del suo piano Danny aveva bisogno di un'ultima cosa prima di compiere il passo successivo, ed era una cosa che non poteva controllare: una tempesta di neve. Madre Natura doveva dargli una piccola spinta sotto forma di un clima tanto schifoso da tenere i dipendenti a casa dall'ufficio.

Nell'inverno del Sud Dakota, lo stato in cui era situata la fabbrica in questione, chi si augurava il maltempo non doveva attendere molto a lungo. Un venerdì sera arrivò la tormenta. Quella che iniziò come una nevicata divenne poi una pioggia gelata, e così al mattino le strade erano glassate da uno strato di ghiaccio sdrucciolevole. Era l'occasione perfetta per Danny.

Telefonò allo stabilimento chiedendo dell'ufficio informatico

in modo da raggiungere un'ape operaia dell'IT, un operatore che si presentò come Roger Kowalski.

Dando il nome del vero dipendente che aveva scovato da qualche parte, Danny disse: "Sono Bob Billings, e lavoro nel Gruppo comunicazioni sicure. Adesso sono a casa e non posso venire in macchina a causa della tormenta. Il problema è che dovrei accedere da casa al mio posto di lavoro e al server ma ho lasciato la Secure ID sulla scrivania. Può recuperarla lei per me? *O* anche un altro? E poi mi legge il codice quando devo entrare? Perché, vede, il mio gruppo ha una scadenza importante e non posso lavorare né venire in ufficio. Quassù le strade sono troppo pericolose".

L'operatore rispose che non poteva lasciare il centro informatico.

Danny allora colse la palla al balzo.

"Lei ce l'ha una Secure ID?"

"Ne abbiamo una qui al centro. Serve per gli operatori in caso di emergenza."

"Senta. Può farmi un grosso favore? Quando faccio il numero per entrare nella rete, mi presta la sua Secure ID? Almeno fino a quando posso venire in macchina."

"Come ha detto che si chiama?" chiese Kowalski.

"Bob Billings."

"Sotto chi lavora?"

"Ed Trenton."

"Ah, lo conosco."

Quando c'è qualche probabilità di trovarsi di fronte una barriera improba da scavalcare, l'ingegnere sociale in gamba fa ricerche più approfondite del solito. "Sto al secondo piano, vicino a Roy Tucker," aggiunse allora Danny.

L'altro conosceva anche quel nome. Danny batté il ferro finché era caldo. "Sarebbe molto più semplice se andasse alla scrivania per riportarmi la mia Secure ID."

Danny era abbastanza sicuro che l'altro non avrebbe abboccato. Intanto non voleva staccarsi dalla postazione in pieno turno per salire in un settore lontano dell'edificio, e poi non gli garbava di andare a frugare nella scrivania di un altro, violando uno spazio privato. No, era da immaginare che non avrebbe accettato.

Kowalski non voleva dire di no a uno che aveva bisogno di una mano, ma nemmeno dire di sì e mettersi nei pasticci, perciò prese tempo dicendo che avrebbe chiesto al suo capo. Posò il ricevitore, quindi Danny lo sentì sollevare un'altra cornetta e spiegare la richiesta. Poi Kowalski fece una cosa incomprensibile, garantì per il presunto Bob Billings, dicendo al suo superiore: "Lo conosco. Lavora per Ed Trenton. Possiamo lasciargli usare la Secure ID del centro?". Danny, sempre in attesa, era stupito di

udire questo imprevisto, incredibile aiuto alla sua causa. Non credeva alle sue orecchie o alla fortuna sfacciata che aveva.

Dopo qualche secondo Kowalski tornò in linea dicendo che il direttore voleva parlare con lui, dandogli nome e numero di telefono.

Danny chiamò e ripeté la storia, aggiungendo anche qualche dettaglio sul progetto su cui stava lavorando e spiegando come mai la squadra aveva questa scadenza. "Sarebbe più semplice andare a prendere la mia card. Non credo che la scrivania sia chiusa a chiave. Dovrebbe essere nel primo cassetto di sinistra."

"Mah, credo che possiamo lasciarle usare quella qui del centro ma solo per il fine settimana. Dico al ragazzo di servizio che quando lei chiama devono leggerle il codice random," disse il direttore, dandogli il PIN allegato.

Per tutto il weekend ogni volta che Danny voleva entrare nel sistema aziendale doveva solo chiamare il centro informatico chiedendo che gli leggessero le sei cifre sulla macchinetta **Secure** ID.

Un lavoro all'interno

Una volta dentro il sistema cosa fare? Come trovare la strada al server contenente il programma che cercava?

Era pronto anche a questo.

Molti utenti delle reti conoscono i newsgroup, quel vasto panorama di BBS dove la gente può porre domande a cui altri risponderanno, oppure trovare compagni virtuali con un comune interesse nella musica, nei computer o in migliaia di altri argomenti.

Quello che pochi capiscono quando mandano un messaggio a un newsgroup è che esso resta in Rete per lustri. Per esempio, Google conserva un archivio con settecento milioni di messaggi, alcuni vecchi di vent'anni! Danny iniziò andando all'indirizzo http://groups.google.com.

Digitò come termini della ricerca "codifica trasmissioni radio" e il nome dell'azienda, trovando un vecchio messaggio di un dipendente, risalente al periodo in cui stavano sviluppando il prodotto, probabilmente molto prima che poliziotti e agenzie federali pensassero di fare lo scrambling dei segnali radio.

Il messaggio era firmato Scott Press, e c'erano anche il numero di telefono e addirittura il nome del collettivo di lavoro, Gruppo comunicazioni sicure.

Afferrò il telefono e compose il numero. Sembrava azzardato. Possibile che quel Press lavorasse ancora lì? Era in ufficio con quel maltempo nel weekend? Dopo tre squilli rispose una voce: "Sono Scott".

Spacciandosi per un impiegato del settore IT dell'azienda, Danny si lavorò Press (secondo modalità che vi sono ormai familiari dai precedenti capitoli) in modo che svelasse i nomi dei server usati per lo sviluppo. Erano quelli che dovevano in teoria conservare il codice sorgente contenente l'algoritmo proprietario e il firmware usato nei prodotti "radio sicura" dell'azienda.

Danny era sempre più vicino, e sempre più eccitato. Stava già pregustando il picco di adrenalina che sentiva sempre quando riusciva in un'impresa fattibile solo da un limitatissimo numero di persone.

Però non era ancora arrivato al traguardo. Per il resto del fine settimana sarebbe potuto entrare nella rete aziendale quando gli pareva grazie a quell'amichevole direttore del centro informatico. E sapeva a quali server accedere. Ma quando componeva il numero, il terminale non gli permetteva di connettersi ai sistemi sviluppo del Gruppo comunicazioni sicure. Doveva esserci un firewall interno o un router a protezione dei sistemi del gruppo. Doveva tentare un'altra strada.

Per la prossima mossa serviva fegato. Danny richiamò Kowalski lamentandosi che il suo server non gli permetteva di collegarsi e che aveva bisogno che l'altro gli aprisse un account su un computer del suo settore per connettersi al sistema in Telnet.

Il direttore aveva già accettato di rivelare il codice d'accesso mostrato dalla macchinetta a tempo, perciò questa nuova richiesta non sembrava campata per aria. Kowalski garantì un account temporaneo e una password su un computer della centrale operativa, consigliando a Danny di richiamare quando non gli fosse servito più, in modo tale da cancellarlo.

Adesso Danny poteva collegarsi alla rete informatica del Gruppo comunicazioni sicure. Dopo un'ora di ricerche di un punto vulnerabile che gli permettesse l'accesso al server principale dello sviluppo, fece centro. A quanto pareva l'amministratore di rete o di sistema non si tenevano aggiornati sui buchi nel sistema operativo che permettevano l'accesso remoto. Invece Danny sì.

In un lampo localizzò i file del codice sorgente che cercava e li trasferì in un sito di e-commerce che offriva spazio gratis. Anche se i file fossero stati scoperti presso quel sito sarebbe stato impossibile risalire a lui.

Era necessario un ultimo passo prima di uscire: la cancellazione metodica delle sue tracce. Finì prima che terminasse lo show serale di Jay Leno. Gli sembrava di avere svolto un proficuo fine settimana di lavoro, e non aveva mai corso rischi personali. Era un'emozione intossicante, anche meglio del paracadutismo o dello snowboard.

Quella sera Danny si ubriacò, non con liquori o birra o saké

ma con la sensazione di onnipotenza mentre controllava i file rubati, avvicinandosi allo sfuggente software radio supersegreto.

Analizziamo l'attacco

Come nella storia precedente, questo attacco ha funzionato perché un dipendente è stato troppo disponibile ad accettare per oro colato che chi aveva al telefono fosse chi sosteneva di essere. Questa disponibilità ad aiutare un collega nei guai da un lato lubrifica gli ingranaggi dell'industria e rende i dipendenti di una ditta colleghi più piacevoli di quelli delle aziende rivali. Ma d'altro canto può rivelarsi una grossa debolezza che un ingegnere sociale tenterà di sfruttare.

Un passaggio della manipolazione di Danny è stato delizioso: quando ha chiesto di andargli a prendere la SecureID dalla scrivania ha usato il termine "riportare", come se si trattasse dell'ordine dato a un cane. Nessuno vuole sentirsi dire una cosa del genere, e con quella parola Danny ha fatto in modo che la richiesta fosse accantonata a favore di altre soluzioni, che era appunto quanto voleva.

L'operatore del centro informatico, Kowalski, ha abboccato ai nomi di gente che conosceva. Ma perché il suo *superiore,* un direttore di settore IT, addirittura, ha permesso a un estraneo di accedere alla rete interna? Semplicemente perché la richiesta di aiuto può essere un'arma potente e persuasiva nell'arsenale dell'ingegnere sociale.

Può succedere una cosa del genere nella *vostra* azienda? È già successa?

> Questa storia vuole dimostrare quanto gli strumenti a tempo e simili forme di autentica non costituiscano una difesa valida contro lo scaltro ingegnere sociale. L'unica difesa sta nel lavoratore coscienzioso che applica le politiche di sicurezza e sa come gli altri possono influenzare in senso negativo il suo comportamento.

PREVENIAMO GLI ATTACCHI

Sembra un elemento ricorrente di questi esempi: l'attaccante riesce a entrare nella rete informatica da fuori senza che la persona che l'aiuta verifichi se è davvero un dipendente autorizzato all'accesso. Perché batto tanto su questo tema? Perché è davvero un fattore decisivo in tanti attacchi. E il modo più semplice per arrivare alla meta. Perché dovrebbero perdere ore a cercare di bucare il sistema quando basta una telefonata?

Uno dei mezzi più efficaci per sferrare questo tipo di attacco è il semplice trucco di fingere di avere bisogno di una mano, una tattica usata di frequente. Non volete certo impedire ai vostri dipendenti di essere utili a colleghi e clienti, perciò dovrete armarli di specifiche procedure di verifica da usare con chiunque presenti una richiesta di accesso ai computer o alle informazioni riservate. In questo modo potranno essere utili a chi si merita di essere aiutato, ma nello stesso tempo proteggeranno le informazioni e i sistemi informatici della struttura.

Le procedure di sicurezza dell'azienda devono esporre in dettaglio il tipo di meccanismi di verifica da usare in varie circostanze. Il *Vademecum* fornirà una lista dettagliata di procedure, ma ecco alcune linee guida su cui riflettere:

- Un ottimo modo per verificare l'identità di una persona che presenta una richiesta è chiamare il numero di telefono che compare nell'elenco dell'azienda. Se chi fa la richiesta è un attaccante la chiamata di verifica vi permetterà di parlare alla vera persona, mentre l'impostore è in attesa, oppure vi permetterà di ascoltare sulla segreteria la sua vera voce da raffrontare con quella dell'attaccante.
- Se la vostra azienda usa i numeri di matricola dei dipendenti come verifica dell'identità, allora dovranno essere trattati come informazioni chiave, da conservare con attenzione e lontane dagli estranei. Altrettanto vale per tutti gli altri generi di identificatori aziendali come i numeri di telefono interni, gli identificatori di spesa di settore e persino gli indirizzi e-mail.
- La preparazione aziendale dovrà richiamare l'attenzione di tutti sulla pratica comune di accettare perfetti sconosciuti come dipendenti legittimi basandosi solo sul fatto che sembrano informati e sicuri di sé. Soltanto perché qualcuno conosce gli usi di una ditta o utilizza la terminologia interna non c'è motivo di dare per scontato che non bisogna verificare la sua identità.
- I responsabili della sicurezza e gli amministratori di sistema non devono restringere la vigilanza in modo da stare solo attenti a quanto *gli altri* sono consapevoli della sicurezza. Anche loro devono essere certi di rispettare le medesime regole e procedure.
- Owiamente le password e simili non devono essere mai condivise, ma le restrizioni sono ancor più importanti con gli strumenti a tempo e le altre forme sicure di autenticazione. Dovrebbe essere ovvio che svelare i dati di uno di questi marchingegni vanifica la stessa installazione di questi sistemi. Condividere significa che non ci sono più persone re-

sponsabili. Se avviene un incidente di sicurezza o qualcosa va storto, non potrete più capire chi è stato.

- Come ripeto in tutto il libro, i dipendenti devono essere pratici delle strategie e dei metodi dell'ingegneria sociale in modo da valutare consapevolmente le richieste che ricevono. Considerate anche se sia il caso di usare i giochi di ruolo come elemento standard dell'addestramento alla sicurezza.

7.
Siti civetta e allegati pericolosi

Un vecchio adagio vuole che non si ottenga mai nulla per nulla. Però il trucco di offrire qualcosa gratis è ancora una grossa esca sia per gli affari legittimi ("Aspetti, non è finita! Se chiama subito aggiungiamo un set di coltelli e la macchina per fare i popcorn!") e meno legittimi ("Se compra un ettaro di palude in Florida gliene diamo un secondo gratis!").

E molti di noi sono tanto contenti quando ottengono qualcosa gratis che rischiano di farsi distrarre da una chiara analisi dell'offerta o della promessa. Conoscete tutti il familiare awertimento "caveat emptor", però adesso è il momento di lanciare un altro monito: attenti agli allegati della posta elettronica e al software gratuito. L'attaccante .esperto userà tutti i mezzi per entrare nella rete aziendale, compreso l'appello al nostro desiderio naturale di ricevere regali. Ecco qualche esempio.

"NON VORREBBE UN (VIRUS) GRATIS?"

Come i virus sono stati un flagello per umanità e medici sin dall'alba della storia, così i loro omonimi informatici rappresentano un flagello paragonabile per chi usa la tecnologia. I virus informatici che suscitano maggiori attenzioni e finiscono sotto i riflettori sono ovviamente quelli che fanno più danni. Sono il prodotto di vandali informatici.

Questi nerd diventati cattivi, questi vandali si fanno in quattro per mostrare quanto sono in gamba. Certe volte le loro imprese sono puri rituali di iniziazione per impressionare hacker più vecchi ed esperti. Questa gente ha un qualche suo motivo recondito per creare un worm o un virus inteso a infliggere danni. Se riescono a distruggere file, interi hard disk e a spedire vi-

rus per posta elettronica a migliaia di vittime inconsapevoli, i vandali si vantano delle loro imprese. Se poi il virus causa abbastanza caos da finire sui giornali e nei notiziari, tanto meglio.

Si è scritto parecchio sui vandali e sui loro virus. Libri, programmi e intere aziende sono nati per offrire protezione, e in questa sede non parleremo delle difese contro gli attacchi in senso tecnico. Per il momento siamo maggiormente interessati agli sforzi più mirati del lontano cugino ingegnere sociale che alle attività distruttive dei vandali.

È arrivato per posta elettronica

Probabilmente ricevete ogni giorno e-mail con richieste contenenti pubblicità o offerte gratis. Sapete come funziona. Vi promettono consigli su come investire, sconti su computer, televisori, macchine fotografiche, vitamine o viaggi, offerte di carte di credito inutili, un aggeggio che vi fa vedere gratis la pay-tv, mezzi per migliorare la salute o la vita sessuale ecc.

Però ogni tanto spunta l'offerta di qualcosa che vi attira. Magari un gioco gratis, la foto della star preferita, un programma calendario gratuito o uno shareware poco costoso per proteggere il vostro computer dai virus. Come che sia, l'e-mail vi indica di scaricare il file contenente l'esca che il messaggio vi ha convinti a provare.

O forse ricevete un messaggio con l'intestazione che dice "Don, mi manchi tanto", o "Anna, perché non mi scrivi più?" o "Ciao, Tim, ecco le foto porno che ti avevo promesso". Pensate che non è junk mail perché reca il vostro nome e sembra personale, quindi aprite l'allegato per vedere la foto o leggere il messaggio.

Tutti questi gesti, scaricare software di cui avete saputo da una e-mail pubblicitaria, cliccare su un link che vi porta in un sito mai sentito, aprire un allegato arrivato da uno che non conoscete sul serio, significano andare in cerca di guai. Certo, quasi sempre quel che ricevete è quel che vi aspettavate, o al massimo è deludente o offensivo ma innocuo. Però ogni tanto vi arriva l'opera di un vandalo.

Inviare codici perniciosi al vostro computer è solo una piccola parte dell'attacco. L'attaccante ha bisogno di convincervi a scaricare l'allegato.

Le forme più dannose di codice maligno, worm con nomi tipo Love Letter, Sircam e Anna Kournikova, tanto per dirne qualcuno, basano tutta la loro diffusione su tecniche di ingegneria sociale di inganno e sfruttamento del nostro desiderio di avere qualcosa in cambio di nulla. Il verme arriva come allegato di

Attenti ai nerd che propongono regali, se non volete che la vostra azienda subisca lo stesso destino della città di Troia. Nel dubbio, per evitare le infezioni, tenete alta la guardia.

una e-mail che offre una tentazione allettante, tipo informazioni riservate, pornografia gratis oppure, trucco assai astuto, un messaggio che dice che l'allegato è la ricevuta di un oggetto costoso che avreste ordinato. Quest'ultimo trucco vi spinge ad aprire l'allegato nel timore che abbiano addebitato sulla vostra carta di credito un acquisto mai fatto.

È incredibile quanta gente ci caschi: anche dopo che ci hanno ripetuto mille volte i rischi di aprire gli allegati delle e-mail, la consapevolezza dei pericoli svanisce con il tempo, lasciandoci tutti più vulnerabili.

Individuare il software ostile

Un altro genere di *malware,* software maligno, infila nel vostro computer un programma che opera senza che lo sappiate o desideriate, oppure esegue un task (compito) senza che ne siate consapevoli. Il *malware* può sembrare innocente, presentandosi addirittura come documento in Word o PowerPoint o qualsiasi programma che abbia una funzionalità macro, ma in segreto installerà un programma non autorizzato. Per esempio, il *malware* può essere una versione del cavallo di Troia discusso nel capitolo *6.* Una volta che il software è installato nel vostro computer può inviare ogni vostra digitazione all'attaccante, comprese tutte le vostre password e numeri di carta di credito.

Ci sono altri due generi di *malware* che potreste trovare scioccanti. Uno può fornire all'attaccante ogni parola che pronunciate nei pressi del microfono del computer, *anche quando siete convinti che il microfono sia disattivato.* Ancor peggio, se avete una webcam collegata al computer, un attaccante che usi una variante di questa tecnica potrà catturare quello che avviene di fronte al vostro terminale anche quando credete che la camera sia spenta, giorno o notte che sia.

Un hacker provvisto di senso dell'umorismo deviato potrebbe tentare di piazzare sul vostro computer un programmino pensato solo per scocciare. Per esempio, potrebbe indurre il vassoio CD ad aprirsi di continuo o il file su cui state lavorando a rimpicciolirsi. Altrimenti potrebbe far sì che un file audio rimbombi al massimo del volume in piena notte. Non è per nulla divertente quando state cercando di dormire o lavorare... ma almeno non causa danni duraturi.

Però le alternative possono essere ben peggiori nonostante tutte le precauzioni che potete prendere. Pensate: avete deciso che non volete correre rischi e che non scaricherete più file se non da siti sicuri di cui vi fidate come SecurityFocus.com o Amazon.com. Non cliccate più sui link nella posta proveniente da fonti sconosciute. Non aprite più allegati da messaggi che non vi aspettavate. E controllate la pagina del browser per verificare che ci sia il simbolo di sito sicuro in ogni sito che visitate per le transazioni di e-commerce o per scambiare informazioni riservate.

E poi un giorno ricevete da un amico o collaboratore una e-mail che contiene un attachment. Può essere forse pericoloso se proviene da uno che conoscete? No. Soprattutto se sapete a chi dare la colpa se il computer subisce dei danni.

Aprite l'allegato e... BUM! Siete stati colpiti da un worm o da un cavallo di Troia. Perché uno che conoscete vi ha fatto una cosa del genere? Perché le cose non sono quel che sembrano. Ne avrete sentito parlare: il verme entra in un computer e poi si spedisce da solo a tutti coloro che compaiono nell'elenco di indirizzi. Ciascuno di loro riceve una e-mail da una persona che conosce e di cui si fida, e invece ogni messaggio fidato contiene il worm che in quel modo si propaga come le onde quando un sasso cade in uno stagno.

Questa strategia è tanto efficace perché segue la teoria dei due piccioni con una fava: la possibilità di propagazione ad altre vittime ignare e la parvenza che sia tutto scaturito da una persona fidata.

È triste, ma allo stato attuale della tecnologia potete ricevere una e-mail da una persona nota e chiedervi ugualmente se sia sicuro aprirla.

> L'uomo ha inventato tante cose meravigliose che hanno cambiato il mondo e la nostra vita, ma per ogni utilizzo benigno della tecnologia, che sia computer, telefono o Internet, qualcuno troverà sempre la maniera di abusarne per i propri interessi.

VARIAZIONI SUL TEMA

Nell'era di Internet c'è una nuova frode che consiste nel dirottarvi verso un sito web che non vi aspettate. Succede di continuo, e in svariate forme. Questo esempio, basato su una vera truffa perpetrata su Internet, è emblematico.

Buon Natale...

Edgar, un agente delle assicurazioni in pensione, ricevette una mail da PayPal, una struttura che offre una maniera veloce e conveniente per effettuare pagamenti online. Questo genere di servizio è utile specialmente quando una persona di una parte del paese (o del mondo) compra un oggetto da un individuo che non conosce. PayPal addebita sulla carta di credito dell'acquirente e poi trasferisce i soldi direttamente sul conto del venditore.

Edgar, collezionista di boccette di vetro antico, faceva molti scambi su eBay, noto sito di aste in rete, e usava spesso PayPal, anche più volte alla settimana, perciò non rimase indifferente quando sotto le feste del 2001 ricevette una e-mail che sembrava arrivare da PayPal e gli offriva un premio se rinnovava il contratto. Il messaggio diceva così:

> Auguri, prezioso cliente di PayPal;
>
> Con l'arrivo del nuovo anno PayPal vorrebbe donarti un credito di 5 dollari sul tuo conto!
> Per incassarlo devi solo aggiornare le informazioni sul nostro sito sicuro PayPal entro il primo gennaio 2002. Un anno porta tanti cambiamenti, e aggiornando i tuoi dati ci permetterai di fornirti il nostro prezioso servizio clienti e intanto avere i dati corretti!
> Per aggiornare le informazioni subito e ricevere istantaneamente i 5 dollari sul tuo conto PayPal, clicca su questo link:
> http://www.paypal-secure.com/cgi-bin
> Grazie per aver usato PayPal.com e averci aiutati a diventare i primi del settore!
> Ti auguriamo sinceramente un buon Natale e felice anno nuovo.
>
> La squadra di PayPal

Edgar non si accorse dei tanti segnali premonitori che indicavano qualcosa di strano in quella e-mail (per esempio, il punto e virgola dopo la prima riga e la formulazione pasticciata) e cliccò, inserendo le informazioni richieste (nome, indirizzo, numero di telefono e dati sulla carta di credito), poi attese che i cinque dollari di credito apparissero nel successivo resoconto della carta. Invece comparve una serie di acquisti di oggetti mai comprati.

Nota sui siti web di commercio elettronico

Immagino conosciate tante persone riluttanti a comprare beni in Rete, anche da compagnie note come Amazon e eBay, o sui siti web di Nike o simili. In un certo senso hanno ragione. Se il vostro browser usa la cifratura a 128-bit l'informazione che inviate a un

sito sicuro esce codificata dal vostro computer e questo dato può essere decrittato soltanto con sforzi erculei, ma più probabilmente non potrà essere decodificato in un tempo ragionevole se non da parte della National Security Agency (che per quanto ne sappiamo non è interessata a rubare numeri di carte di credito o scoprire chi ordina cassette porno o biancheria erotica).

Questi file cifrati possono essere decodificati da uno che abbia tempo e mezzi, però nessuno sarebbe tanto sciocco da fare tanta fatica per rubare un numero di carta di credito quando ci sono tante ditte di e-commerce che commettono l'errore di conservare le informazioni sui loro clienti non cifrate nei database. Ancor peggio, parecchie strutture di e-commerce che usano un particolare programma database SQL aggravano il problema così: non hanno mai cambiato la password di default dell'amministratore di sistema del software. Quando hanno estratto i dischetti dalla scatola la password era "null", e lo è ancora oggi, quindi i contenuti del database sono alla mercé di chiunque in Internet decida di volersi connettere al server del database. Questi siti sono sottoposti ad attacchi continui e le informazioni sono rubate senza che nessuno capisca l'antifona.

D'altro canto, gli stessi che non comprerebbero mai su Internet per paura che gli rubino i dati della carta di credito non hanno problemi a usare la medesima carta in un negozio normale o per pagare al ristorante, persino in locali equivoci dove non porterebbero la mamma. In questi esercizi le ricevute di carta di credito sono rubate un giorno sì e un giorno no, oppure vengono recuperate dal pattume. E qualsiasi commesso o cameriere poco onesto può trascrivere nome e numero o usare un marchigegno, facilmente reperibile in Internet, che conserva i dati per un controllo successivo.

Certo, ci sono dei rischi a comprare in Rete, però è sicuro quanto comprare in un negozio normale. E le compagnie di emissione vi offrono la stessa protezione per l'utilizzo in Rete: se ci sono stati addebiti fraudolenti siete responsabili solo dei primi cinquanta dollari.

Quindi, secondo me, la paura di comprare in Rete è ingiustificata.

Per quanto non sia comunque a prova di bomba (nessuna protezione lo è), quando visitate un sito che vi chiede informazioni che ritenete personali assicuratevi sempre che la connessione sia autenticata e cifrata. Ancor più importante, non cliccate automaticamente "**Sì**" in una finestra di dialogo relativa a un problema di sicurezza, per esempio quando un certificato digitale è scaduto, non più valido e revocato.

Analizziamo l'attacco

Edgar è caduto in un classico raggiro internettiano, che si presenta in vari modi. Uno di questi (spiegato nel capitolo 9) prevede una falsa schermata di log-in che sembra identica a quella vera, solo che non dà accesso al sistema che l'utente vuole raggiungere ma passa invece all'hacker username e password.

Edgar è stato coinvolto in una truffa in cui i lestofanti avevano registrato un sito web come "paypal-secure.com", che suonava come una pagina sicura del legittimo sito PayPal, e invece non lo era. Quando ha inserito le informazioni in quel sito gli attaccanti hanno ottenuto quanto cercavano.

VARIAZIONI SULLA VARIAZIONE

Quanti altri modi ci sono per ingannare un utente in modo che vada su un sito web fasullo dove lascerà informazioni riservate? Non credo che nessuno abbia una risposta valida, però "un sacco" rende l'idea.

L'anello mancante

C'è un trucco diffusissimo: inviare una e-mail che offre un motivo stuzzicante per visitare un sito e fornisce il link per andarci direttamente. Peccato che il link non ti porta al sito che credi perché la grafia è solo somigliante. Ecco un altro esempio realmente usato in Internet, che anche in quèsto caso riguarda l'uso improprio del nome PayPal:

www.PayPai.com

Di primo acchito sembra esserci scritto PayPal, ma anche se la vittima se ne accorge può pensare che sia soltanto un piccolo difetto nel testo che fa sembrare la elle una i. E chi mai può notare che

www.PayPa1.com

usa un numero invece della lettera l minuscola? Le persone che accettano refusi e altri errori sono abbastanza numerose da rendere questo trucchetto ancora popolarissimo tra i banditi delle carte di credito. Quando le vittime vanno nel sito fasullo, esso sembra quello che si aspettano, quindi allegramente inseri-

scono le informazioni della loro carta. Per organizzare una di queste truffe l'attaccante ha solo bisogno di un dominio dal nome simile, di inviare le e-mail e aspettare che gli ingenui abbocchino, pronti a essere ingannati.

A metà del **2002** ho ricevuto una e-mail che sembrava far parte di un mass mailing proveniente da "Ebay@ebay.com". Compare nella figura 8.1.

Le vittime che hanno cliccato sul link sono finite in una pagina web somigliante a una pagina eBay. In effetti era ben progettata, con un autentico marchio eBay, e tutti i link "Browse", "Sell" eccetera che una volta cliccati portavano il visitatore al vero sito eBay. C'era anche un logo di sicurezza nell'angolo in basso a destra. Per ingannare anche le vittime più astute il progettista aveva usato un crittaggio HTML per nascondere dove veniva inviata l'informazione fornita dall'utente.

Era un eccellente esempio di attacco ostile tramite computer, però non era esente da pecche.

Il messaggio non era ben formulato, soprattutto il paragrafo che iniziava con "Riceve questo avviso" era goffo e confuso (i responsabili di queste truffe non ingaggiano mai un professionista che gli elabori la copia, e si nota sempre). Inoltre, se uno si fosse soffermato a pensare un attimo avrebbero trovato un po' sospetto che eBay chiedesse i dati PayPal del visitatore. Non c'è alcun motivo per cui eBay debba chiedere a un cliente dati riservati che riguardano un'azienda diversa.

E chiunque conosca Internet nota che l'hyperlink non connette al dominio eBay bensì a tripod.com, che è un servizio di siti

Msg: Caro cliente eBay,
è stato osservato che un'altra parte sta corrompendo il suo account eBay e ha violato la nostra politica Contratto utente elencata come:

4. Offerte e acquisti

Lei è obbligato a completare la transazione con il venditore se acquista una voce tramite uno dei nostri pacchetti a prezzo fisso oppure è il più alto offerente come descritto sotto. Se è il più alto offerente alla fine dell'asta (rispettando l'offerta minima) e la sua offerta è accettata dal venditore, sarà obbligato a completare la transazione, oppure la transazione sarà proibita ai sensi della legge o di questo contratto.
Riceve questo avviso da eBay perché è giunto alla nostra attenzione che il suo account attuale ha causato interruzioni presso altri soci eBay, ed eBay richiede immediata verifica del suo account. La preghiamo quindi di verificarlo se non vuole che sia disabilitato. Clicchi Qui Per Verificare Il Suo Account – http://error_ebay.tripod.com
I trademark e marchi designati sono proprietà dei loro rispettivi detentori. eBay e il logo eBay sono marchi registrati di eBay Inc.

***Figura* 7.1 Il link in questa o altre e-mail dovrebbe essere usato con estrema cautela.**

web gratuiti. Era la prova definitiva che non si trattava di una mail onesta. Però scommetto che un sacco di gente ha inserito quelle informazioni sulla pagina, compreso il proprio numero di carta di credito.

State attenti

Come utenti singoli di Internet, dobbiamo stare tutti attenti, decidendo con lucidità quando è sensato inserire dati personali, password, numeri di conto, PIN e simili.

Quanta gente conoscete in grado di dirvi se una qualunque pagina Internet che sta guardando è sicura? Quanti dipendenti della vostra azienda sanno che cosa cercare?

Tutti coloro che usano Internet dovrebbero sapere del simbolino che spesso compare in una pagina web e somiglia a un lucchetto. Dovrebbero sapere che quando esso è chiuso il sito è certificato sicuro, quando invece è aperto o manca del tutto l'icona allora il sito web non è autenticato come genuino e ogni informazione trasmessa si troverà alla luce del sole, cioè decodificata.

Comunque un attaccante che riesce a compromettere i privilegi amministrativi su un computer aziendale può essere in grado di manipolare il codice del sistema operativo in modo da cambiare la percezione di quanto succede. Per esempio, le istruzioni di programmazione nel browser che indicano la non validità del certificato digitale di un sito web possono essere modificate in modo da bypassare il controllo. Oppure il sistema può essere modificato con un cosiddetto "root kit", installando una o più *backdoors* a livello del sistema operativo, più difficili da individuare.

Una connessione sicura autentica il sito come genuino e codifica le informazioni comunicate di modo che un attaccante non possa usare i dati intercettati. Potete fidarvi di un sito web, almeno di uno che utilizza una connessione sicura? No, perché forse il proprietario del sito non è attento a tutti gli adeguamenti di sicurezza necessari, né costringe gli utenti o gli amministratori a rispettare il corretto uso delle password. Perciò non potete dare per scontato che un sito in teoria sicuro sia invulnerabile.

Un HTTP (hypertext transfer protocol) o SSL (secure sockets layer) sicuro fornisce un meccanismo automatico che sfrutta i certificati digitali non solo per cifrare le informazioni inviate al sito remoto ma anche per autenticare (l'assicurazione che state comunicando con il vero sito web). Purtroppo questa protezione non funziona con gli utenti che non prestano attenzione se il

nome del sito che compare nella barra dell'indirizzo è proprio quello cui vogliono accedere.

Un altro problema della sicurezza spesso ignorato compare come un messaggio che dice più o meno: "Questo sito non è sicuro oppure il certificato di sicurezza è scaduto. Vuoi entrare ugualmente?". Molti utenti di Internet non capiscono, e quando compare il messaggio cliccano "Sì" oppure proseguono con il loro lavoro senza sapere che procedono sulle sabbie mobili. Attenti: in un sito web che non usa un protocollo sicuro, non dovete mai inserire informazioni riservate come indirizzo o numero di telefono, numeri di carta di credito o di conto corrente o altri dati che volete tenere riservati.

Thomas Jefferson diceva che per preservare la libertà occorre "un'eterna vigilanza". Altrettanto dicasi per salvaguardare la privacy e la sicurezza in una società che usa le informazioni come moneta corrente.

Consapevoli dei virus

Una nota speciale sul software contro i virus: è fondamentale per l'intranet aziendale ma anche per ogni dipendente che usa il computer. Oltre ad avere installato un antivirus, gli utenti devono chiaramente avere il software attivato (a molti non piace perché inevitabilmente rallenta le funzioni).

Con l'antivirus dovete tenere presente anche un'altra procedura importante: tenere aggiornate le definizioni dei virus. A meno che la vostra azienda non sia organizzata in modo da distribuire programmi o aggiornamenti in rete a ogni utente, ogni singolo deve essere responsabilizzato a scaricare le ultime serie di definizioni dei virus. La mia raccomandazione personale è far sì che tutti impostino le preferenze del programma in modo che le definizioni dei virus siano aggiornate in automatico tutti i giorni.

In parole povere, siete ancora vulnerabili se le definizioni non sono aggiornate con regolarità. E non siete comunque al sicuro da virus e worms che i produttori di antivirus non conoscono ancora o per cui non hanno ancora pubblicato un file di rilevamento del pattern virale.

Tutti i dipendenti con privilegi di accesso remoto dal portatile o dal personal devono essere come minimo forniti di un antivirus aggiornato e di un firewall personale per la macchina. Un attaccante sofisticato guarderà il panorama completo in cerca dell'anello debole, per attaccare in quel punto. Ricordare di continuo ai dipendenti con un computer remoto la necessità di firewall personali e programmi antivirus aggiornati e attivati è una

responsabilità dell'azienda perché non potete pretendere che i singoli dipendenti, dirigenti, rappresentanti e altri lavoratori esterni al settore IT si ricordino dei pericoli del computer non protetto.

Oltre a ciò, raccomando con forza l'uso dei pacchetti software meno comuni ma non meno importanti contro i cavalli di Troia, i cosiddetti "software anti-Trojan". Mentre scrivo, due dei migliori sono The Cleaner (www.moosoft.com) e Trojan Defense Sweep (www.diamondcs.com.au).

Per finire, il messaggio riguardante la sicurezza forse più importante per tutte le aziende che non controllano le e-mail pericolose al gateway: visto che tendiamo tutti a dimenticarci o a trascurare cose che sembrano marginali per il nostro lavoro, dovete ricordare in continuazione ai dipendenti, in tanti modi, di non aprire mai gli allegati a meno che non siano sicuri che la fonte è persona o struttura fidata. E la direzione deve anche ricordare ai dipendenti che devono usare antivirus e anti-Trojan attivi, una protezione inestimabile contro le e-mail apparentemente affidabili che possono contenere un carico dinamitardo.

8.

Sfruttare simpatia, senso di colpa e intimidazione

Come vedremo nel capitolo 15, l'ingegnere sociale sfrutta la psicologia per indurre la vittima a cedere alle sue richieste. I più abili sono molto bravi a impostare un raggiro che susciti emozioni tipo paura, eccitazione o senso di colpa, e ci riescono facendo scattare dei pulsanti psicologici, dei meccanismi automatici che inducono le persone a rispondere alle richieste senza fare un'analisi approfondita di tutte le informazioni disponibili.

Tutti quanti preferiamo evitare le situazioni spinose per noi e per gli altri. Basandosi su questa motivazione positiva, l'attaccante può giocare sulla pietà di una persona, farla sentire colpevole oppure usare come arma l'intimidazione.

Ecco qualche lezioncina sulle più diffuse tattiche che giocano sulle emozioni.

UNA VISITA AGLI STUDI

Avete mai notato che c'è gente che può andare dal buttafuori, che so, di una sala da ballo in cui è in corso una festa o un'assemblea o il lancio di un libro ed entrare senza che le chiedano nemmeno un biglietto o un invito?

È più o meno in questo modo che l'ingegnere sociale riesce a intrufolarsi in posti che non riterreste accessibili, come chiarisce la seguente storiella riguardante l'industria cinematografica.

La telefonata

"Ufficio di Ron Hillyard, sono Dorothy."

"Ciao, Dorothy, sono Kyle Bellamy. Sono appena arrivato allo

sviluppo animazioni, nel gruppo di Brian Glassman. Certo che qua fate cose da urlo."

"Credo. Non ho mai lavorato in altri studi perciò non so che dire. Che cosa posso fare per lei?"

"A essere sincero, mi sento un po' stupido. Oggi pomeriggio arriva uno sceneggiatore per una proposta e non so con chi devo parlare per farlo entrare. Qui da Brian sono molto carini però mi dà fastidio disturbarli continuamente per chiedere la minima inezia. Mi sembra di essere quello appena arrivato in una scuola nuova che non sa dov'è il bagno. Non so se mi spiego."

Dorothy scoppia a ridere.

"Deve parlare con la sorveglianza. Faccia il 7, poi 6138. Se parla con Lauren le dica che la manda Dorothy."

"Grazie, Dorothy. E se non trovo il bagno ti richiamo!"

Ridono entrambi alla battuta, poi riattaccano.

La versione di David Harold

Adoro il cinema, e quando sono venuto a Los Angeles m'immaginavo che avrei incontrato tanta gente del mondo della celluloide che mi avrebbe portato alle feste e invitato a pranzo negli studios. Be', dopo un anno ne avevo già compiuti ventisei e il massimo che avevo visto era stata la visita guidata agli studi Universal assieme a tanti turisti simpatici di Phoenix e Cleveland. Così alla fine mi sono detto che se non mi invitavano loro mi sarei invitato da solo. E così ho fatto.

Ho comprato per un paio di giorni il "Los Angeles Times" per leggere la sezione spettacoli, appuntandomi i nomi di alcuni produttori di studi diversi, e ho deciso di colpire subito una grande casa di produzione.

Così ho telefonato al centralino chiedendo l'ufficio di un produttore di cui avevo letto sul giornale. La segretaria che ha risposto sembrava del tipo

> Una volta che l'ingegnere sociale sa come funzionano le cose dentro l'azienda bersaglio, diventa facile usare queste informazioni per far nascere un rapporto con i legittimi dipendenti. Le aziende devono essere preparate agli attacchi da parte di dipendenti o ex con il dente avvelenato. Possono essere utili i controlli sul passato per eliminare i candidati propensi a questo genere di comportamento. Ma nella maggior parte dei casi queste persone sono estremamente difficili da individuare. L'unica salvaguardia ragionevole in questi casi sono le procedure di verifica dell'identità, compreso lo status della persona, prima di rivelare informazioni a chi non è direttamente noto per essere ancora in rapporto con l'azienda.

matronale, perciò ho pensato di aver fatto centro. Se fosse stata una giovane che lavorava lì in attesa di sfondare forse non mi avrebbe prestato attenzione.

Invece, questa Dorothy sembrava una che raccoglieva i gattini randagi, che si rammaricava per il collega nuovo un po' travolto dal nuovo lavoro. E toccai il tasto giusto. Non capita spesso di raggirare qualcuno che ti dà anche più di quel che chiedi. Così, mi diede non solo il nome di una tale della sorveglianza, ma disse che potevo riferire che mi mandava Dorothy.

Avevo già previsto di usare comunque il suo nome, ma in questo modo era ancora meglio. Lauren abboccò e non si premurò nemmeno di controllare nel database dipendenti il nome che diedi.

Quando quel pomeriggio arrivai al cancello avevano il mio nome in lista e anche un posto per parcheggiare l'auto. Mangiai in mensa e mi aggirai negli studi per tutto il giorno, mi intrufolai persino in un paio di teatri di posa mentre giravano. Me ne andai alle sette di sera. È stata una delle giornate più eccitanti della mia vita.

Analizziamo l'attacco

Tutti siamo stati un neoassunto. Tutti ricordiamo com'è stato il primo giorno, soprattutto quando eravamo giovani e inesperti. Perciò quando uno nuovo chiede aiuto si aspetta che tanti colleghi, soprattutto ai livelli più bassi, si ricordino di quei momenti e si facciano in quattro per dargli una mano. L'ingegnere sociale lo sa e ne approfitta per accattivarsi la simpatia delle sue vittime.

Rendiamo troppo agevole agli estranei entrare di soppiatto negli impianti e uffici della nostra azienda. Anche con le guardie ai cancelli e con le procedure di accredito per chi non è del personale, una qualsiasi delle tante varianti del raggiro del precedente aneddoto permetterà all'intruso di procacciarsi un pass. E se la vostra azienda prevede un accompagnatore per i visitatori? Ottima regola, ma efficace solo se i dipendenti sono consapevoli che devono bloccare un visitatore solo soletto, con o senza pass. E se poi le risposte non li soddisfano devono avvertire la sorveglianza.

Se rendete troppo facile per gli esterni entrare nelle vostre strutture mettete in pericolo le informazioni delicate della compagnia. E con l'aria che tira, con la minaccia di attacchi terroristici, i rischi non riguardano solo le informazioni.

Non tutti coloro che usano le tecniche di ingegneria sociale sono ingegneri sociali. Chiunque conosca i segreti di una data azienda può diventare pericoloso. Il rischio è anche maggiore per le aziende che conservano nei file o nei database informazioni riservate sui propri dipendenti, come succede a tante.

Quando i lavoratori non sono preparati a riconoscere gli attacchi degli ingegneri sociali, individui determinati come la giovane arrabbiata della storia seguente possono fare cose che quasi tutti ritengono impossibili.

La versione di Doug

Tanto le cose non andavano più bene con Linda, e appena ho conosciuto Erin ho capito che era quella giusta. Linda è, come dire, un tantino... mah, non instabile, ma quando le gira male esagera.

Le dissi con la massima delicatezza che doveva fare le valigie, poi le diedi una mano e le lasciai persino prendere un paio di dischi dei Queensryche che in realtà erano miei. Appena andò via mi recai in un negozio di ferramenta a comprare una nuova serratura per la porta d'ingresso, che installai la sera stessa. Il giorno dopo feci cambiare il numero di telefono, che non doveva figurare nell'elenco.

Adesso potevo pensare a Erin.

La versione di Linda

Tanto ero già pronta ad andarmene, solo che non avevo deciso quando. Però non piace a nessuno essere cacciati. Quindi adesso mi interessava solo fargli capire che era un verme.

Non ci misi molto a decidere. Doveva esserci di mezzo un'altra, altrimenti non mi avrebbe detto di fare le valigie tanto in fretta. Così avrei aspettato un po' prima di iniziare a chiamarlo sul tardi. Sapete, all'ora in cui non fa piacere essere svegliati.

Aspettai il fine settimana, le undici di sera del sabato. Peccato che aveva cambiato numero, e il nuovo non era nell'elenco. Tanto per confermare che figlio di puttana era quello.

Non era un grosso problema. Iniziai a frugare tra le scartoffie che avevo portato a casa prima di mollare il lavoro all'azienda dei telefoni. Eccolo. Avevo conservato un biglietto della riparazione quando c'era stato un problema con i cavi da Doug, in cui erano elencati i fili del suo telefono. Vedete, potete cambia-

re numero di telefono finché vi pare, però vi serve sempre un paio di fili di rame che corrono da casa vostra fino alla centralina della compagnia dei telefoni [chiamata in gergo "C.O.", Centra1 Office]. I fili che escono da ogni villetta e palazzo sono identificati tramite numeri e se sapete come opera il fornitore del servizio, e io lo so, sono sufficienti per ottenere anche il numero di telefono.

Avevo un elenco di tutti i C.O. in città, con indirizzi e numeri di telefono. Cercai quello più vicino allo stronzo e chiamai, ma naturalmente non c'era nessuno. Dove sono quando ne hai bisogno? Impiegai circa venti secondi per escogitare un piano, poi iniziai a chiamare i vari uffici finché trovai un tecnico, lontano e presumibilmente sfaccendato. Sapevo che non avrebbe fatto quel che volevo. Però ero pronta con il mio piano.

"Sono Linda, Centro riparazioni. Abbiamo un'emergenza. Il servizio dell'unità ambulanze è in tilt. Un tecnico sta cercando di metterci una pezza ma non riesce a trovare il problema. Dovresti andare immediatamente alla centrale di Webster per vedere se esce il segnale," dissi, poi aggiunsi che l'avrei richiamato io una volta giunto lì, perché ovviamente non doveva essere lui a chiamare me al Centro riparazioni.

Sapevo che non aveva affatto voglia di lasciare la comoda sede centrale per grattare il ghiaccio dal parabrezza e infilarsi nel nevischio a quell'ora. Però era un'"emergenza", quindi non poteva obiettare che aveva da fare.

Quando lo raggiunsi alla centrale di Webster 45 minuti dopo gli chiesi di controllare il cavo 29, coppia di fili 2481. Lui andò al quadro e disse che il segnale c'era. Ma questo lo sapevo già.

Allora dissi: "Bene, fammi una verifica linea" [Lv nel gergo telco], cioè gli chiedevo di verificare il numero componendo un numero speciale che legge l'altro senza però segnalare se è riservato o è stato appena cambiato. Perciò il brav'uomo eseguì e io sentii annunciare il numero nel suo apparecchio di collaudo. Fantastico. Era andato liscio come l'olio.

Aggiunsi che il problema doveva essere sul campo, come se il numero lo sapessi da sempre, lo ringraziai e gli garantii che avremmo continuato a lavorarci, poi gli augurai la buona notte.

Alla faccia di Doug e del suo numero riservato. Adesso poteva cominciare lo spasso.

Analizziamo l'attacco

La giovane di questa storia è riuscita ad avere le informazioni che cercava per compiere la sua vendetta perché disponeva di

informazioni dall'interno, cioè i numeri utili, le procedure e il gergo dell'azienda. Così non solo ha trovato un nuovo numero non disponibile al pubblico, ma c'è riuscita in una notte d'inverno spedendo un tecnico dall'altra parte della città.

"LA DESIDERA IL GRAND'UOMO"

Una forma di intimidazione classica ed efficacissima (classica in quanto semplice) si basa sull'uso della posizione gerarchica per influenzare il comportamento delle persone.

Basta il nome dell'assistente dell'amministratore delegato. Gli investigatori privati e i cacciatori di teste lo fanno tutti i giorni, chiamano il centralino chiedendo di passargli l'ufficio del presidente. Quando risponde la segretaria o un vice, dicono che hanno un documento o un pacchetto per il capo. Oppure, se per caso mandano un allegato, possono stamparlo? Altrimenti chiedono il numero di fax. A proposito, come si chiama lei?

Poi chiamano un altro dicendo: "Jeannie dell'ufficio del grand'uomo mi ha detto di chiamarla perché mi dia una mano".

E la tecnica del *name-dropping*, del citare un nome noto, e di solito induce il bersaglio a credere che l'attaccante sia in stretto contatto con una persona autorevole, rendendolo più disponibile a fare un favore a qualcuno che conosce qualcuno che lui conosce.

Se l'attaccante ha preso di mira informazioni riservatissime, può usare questa tattica per suscitare emozioni utili nella vittima, come la paura di essere criticato dai superiori. Ecco un esempio.

La versione di Scott

"Scott Abrams."

"Scott, sono Christopher Dalbridge e ho appena sentito al telefono il signor Biggley che è decisamente di malumore. Sostiene di aver inviato dieci giorni fa un messaggio in cui vi sollecitava a mandarci le copie per l'analisi di tutte le vostre indagini sulla penetrazione di mercato. Non ci è mai arrivato niente."

"Indagini sulla penetrazione di mercato? Nessuno mi ha detto niente. Di che ufficio è lei?"

"Siamo una ditta di consulenza, e siamo già in ritardo."

"Senta, sto per andare a una riunione. Se mi dà il numero di telefono..."

Adesso l'attaccante sembra davvero scocciato. "Devo riferire questo al signor Biggley?! Senta, lui si aspetta la nostra analisi

per domattina e dobbiamo lavorarci stanotte. Vuole che gli dica io che non ci siamo riusciti perché non abbiamo avuto la relazione da lei, oppure preferisce spiegarglielo di persona?"

Un capo arrabbiato può rovinarti la settimana. È assai probabile che la vittima decida che è meglio risolvere l'inghippo prima di andare in riunione. Anche stavolta l'ingegnere sociale ha premuto il tasto giusto per ottenere la reazione che voleva.

Analizziamo l'attacco

Il trucco dell'intimidazione citando un superiore funziona alla grande soprattutto se l'altro è a un livello abbastanza basso della gerarchia. Usare un nome di peso non vince soltanto la normale riluttanza o i sospetti, ma spesso rende ansiosa quella persona di farti un piacere. L'istinto innato che ci spinge a dare una mano si rafforza quando crediamo che la persona che stiamo aiutando sia importante o influente.

Però l'ingegnere sociale sa che in queste specifiche sceneggiate è meglio usare il nome di un boss più in alto del diretto superiore della vittima. Ed è difficile farlo in una piccola organizzazione, perché l'attaccante non vuole che il bersaglio faccia un commento casuale con il vicepresidente del marketing. "Ho poi mandato il piano di marketing che lei voleva spedissi a quel consulente" può produrre facilmente una reazione tipo: "Quale piano? Che consulente?" e ciò porterebbe alla scoperta del colpo tirato all'azienda.

L'intimidazione può creare la paura della punizione, costringendo la gente a collaborare. Inoltre, può anche far nascere la paura dell'imbarazzo o di essere esclusi dalla prossima promozione.
Il personale dev'essere addestrato al fatto che non solo è permesso ma obbligatorio affrontare i superiori quando è in ballo la sicurezza. Il training alla sicurezza delle informazioni dovrebbe prevedere di insegnare come affrontare i superiori in maniera rilassata, senza compromettere il rapporto. Inoltre, tali esigenze devono essere appoggiate dai vertici. Se un dipendente non sarà giustificato perché ha affrontato una persona indipendentemente dalla carica di quest'ultima, la reazione normale è che non lo farà più, esattamente l'opposto di quel che conviene.

QUELLO CHE LA PREVIDENZA SOCIALE SA DI TE

Ci piacerebbe credere che gli enti statali che conservano dati su di noi li tengano al riparo dalla gente che non ha una vera necessità di esserne messa al corrente. In realtà, nemmeno la pub-

blica amministrazione è immune alle penetrazioni come preferiremmo immaginare.

La telefonata a May Linn

Luogo: una sede regionale della previdenza sociale
Ora: 10:18, giovedì mattina

"Mod 2, sono May Linn Wang."
La voce all'altro capo del filo sembra timida, pare quasi scusarsi.
"Signora Wang, sono Arthur Arondale dell'Ispettorato generale. Possiamo darci del tu, May?"
"May Linn."
"Senti, May Linn, c'è qui uno che non ha ancora il computer e adesso che ha un'urgenza sta usando il mio. Siamo il governo degli Stati Uniti però ci ripetono di non avere i soldi in bilancio per dare un computer a quel tale. E adesso il mio capo mi dice che sono in ritardo e non vuole sentire scuse."
"Ti capisco perfettamente."
"Puoi aiutarmi in una ricerca sull'MCS?" chiede lui, citando il sistema informatico per le informazioni sui contribuenti.
"Certo. Che cosa ti serve?"
"Intanto un alphadent su Joseph Johnson, data di nascita 4 luglio '69. (Con alphadent si intende una ricerca alfabetica al computer secondo nome e data di nascita.)"
Dopo una pausa lei chiede: "Cosa vuoi sapere?".
"Il numero."
Lei gli legge il numero della previdenza sociale.
"Bene, adesso un numident sul numero."
È una richiesta dei dati anagrafici del contribuente. May Linn legge luogo di nascita, cognome da ragazza della madre e nome del padre. Il presunto Arthur ascolta paziente anche quando lei gli riferisce mese e anno di rilascio delle tessera e ufficio distrettuale relativo.
Poi chiede una ricerca dettagliata sulle entrate.
"Per quale anno?"
"2001."
May Linn legge: "190.286 dollari, pagati da Johnson Micro Tech.
"Altre fonti di reddito?"
"No."
"Grazie, sei stata molto gentile."
Poi Arthur cerca di mettersi d'accordo con May Linn per poterla interpellare ogni volta che ha bisogno di informazioni e

non può usare il computer, con il trucco preferito dagli ingegneri sociali, cioè cercare di stabilire un rapporto solido per poter fare riferimento alla stessa persona evitando così la rottura di dover trovare ogni volta un nuovo pollo.

"Non la settimana prossima," spiega lei, perché va nel Kentucky al matrimonio della sorella. Però in altri momenti quando vuole.

Mentre appende May Linn è contenta di aver dato una mano a un altro pubblico dipendente poco apprezzato.

La versione di Keith Carter

Se dobbiamo giudicare dai film e dai gialli, un investigatore privato è un tipo privo di morale e ricco di esperienza su come si fa a strappare alla gente notizie con metodi assolutamente illegali ma sempre riuscendo a evitare per un soffio l'arresto. Ovviamente, la realtà è che molti mandano avanti agenzie assolutamente irreprensibili. Visto che quasi tutti hanno cominciato come tutori dell'ordine, sanno perfettamente che cosa è legale e che cosa non lo è, e molti di loro non sono propensi a superare i limiti.

Però ci sono le eccezioni. Alcuni privati, non pochi, corrispondono al cliché dei gialli e sono noti nel giro come broker o mediatori di informazioni, eufemismo per definire chi è disposto a infrangere la legge. Costoro sanno che possono finire il lavoro molto più in fretta se prendono qualche scorciatoia. Il fatto che sia un potenziale reato che può farli finire dietro le sbarre per alcuni anni non sembra scoraggiare i meno scrupolosi.

Di solito gli investigatori privati di lusso, quelli che lavorano in eleganti uffici nei quartieri dagli affitti vertiginosi, non agiscono direttamente ma assoldano un broker di informazioni.

Colui che chiamaremo Keith Carter era appunto il genere di detective privato con poche remore etiche.

Era il classico caso in cui devi scoprire dove lui ha nascosto i soldi. Certe volte è anche: dove lei ha nascosto i soldi. Quasi sempre si tratta di una riccona che vuole sapere dove il marito ha imboscato il denaro che le appartiene (perché mai una donna piena di liquidi debba sposare uno che ne è sprovvisto è un enigma cui Keith Carter non ha mai trovato risposta).

In questo caso era il consorte, Joe Johnson, quello che teneva i soldi in ghiaccio. Joe era un tipo dawero in gamba che aveva fondato una ditta di hi-tech con diecimila dollari gentilmente prestati dalla famiglia della moglie per trasformarla in un'impresa multimilionaria. Secondo l'awocato divorzista della don-

na, il buon Joe era stato molto bravo a nascondere i suoi beni mobili, e adesso il legale voleva il quadro completo.

Keith pensò di partire dalla previdenza sociale, dai loro file su Johnson che sarebbero stati pieni di informazioni utili in una situazione del genere. Poi, armato di questi dati, avrebbe finto di essere il coniuge fedifrago per convincere banche, fondi di investimento e istituti off-shore a spifferargli l'arcano.

La prima telefonata fu fatta a un ufficio locale usando il numero indicato dall'elenco. Quando rispose un impiegato, Keith chiese di passargli qualcuno delle liquidazioni. Altra attesa, poi una voce. A questo punto cambiò tattica. "Salve, sono Gregory Adams, ufficio 329. Senta, sto cercando di trovare un liquidatore con un numero che finisce con 6363, ma mi risponde un fax."

"È il Mod 2," rispose l'impiegato, poi diede il numero a Keith.

A quel punto il nostro eroe chiamò il Mod 2. Quando rispose May Linn lui cambiò parte e inventò la storia dell'Ispettorato generale e di avere il problema che al suo computer c'era un altro. Lei gli diede le informazioni e accettò di aiutarlo in futuro.

> È incredibile quanto sia facile per gli ingegneri sociali convincere la gente sulla base di come impostano la richiesta, innescando una reazione automatica basata sui principi psicologici e sulle scorciatoie mentali che scattano quando una persona percepisce l'interlocutore come un alleato.

Analizziamo l'attacco

Questa tattica è stata tanto efficace perché ha giocato sulla simpatia dell'impiegata con la storia che c'era un altro al suo computer e "il mio capo ce l'ha con me". La gente non mostra molto spesso emozioni sul posto di lavoro, e quando questo capita può fare crollare le normali difese contro gli attacchi degli ingegneri sociali. Il trucco psicologico del farsi aiutare quando si è nei guai è bastato a fare tombola.

Forse l'attaccante non avrebbe ottenuto l'informazione da un impiegato abituato a gestire le chiamate dal pubblico. Il genere di attacco usato da Keith funziona solo quando l'altro ha un numero di telefono ignoto al pubblico e perciò si aspetta che chi chiama sia uno competente (altro esempio di sicurezza in stile speakeasy).

Gli elementi che hanno fatto funzionare questo attacco sono:

- Conoscere il numero di telefono del Mod.
- Conoscere la terminologia usata, numident, alphadent e simili.

- Fingere di essere dell'Ispettorato generale, perché ogni pubblico dipendente sa essere un'agenzia investigativa dotata di ampi poteri. Ciò conferisce all'attaccante un'aura di autorevolezza.

Chiarimento interessante: pare che gli ingegneri sociali sappiano come fare richieste in modo che l'altro non si domandi mai perché ha chiamato proprio ***lui,*** anche quando sarebbe stato logico telefonare a un altro ufficio. Forse aiutare chi chiama offre un tale diversivo alla monotonia del lavoro quotidiano che la vittima non pensa mai quanto è insolita quella chiamata.

Per finire, l'attaccante di questo caso, ancora insoddisfatto dopo avere ottenuto le informazioni per quell'incarico specifico, voleva tenere aperto un contatto regolare. Come alternativa avrebbe potuto usare un trucco comune negli attacchi impietosenti ("Ho versato il caffè sulla tastiera"). Però in questo caso era inutilizzabile perché una tastiera si rimpiazza in un giorno, quindi ha usato la scusa di un altro seduto al suo computer, che poteva reggere per settimane intere. "Già, pensavo che gliel'avrebbero dato ieri, invece la nuova macchina se l'è accaparrata un altro. Così quel buffone siede ancora alla mia scrivania." Eccetera.

"Povero me, ho bisogno d'aiuto." Funziona che è una bellezza.

Insicurezza sociale

Voi non ci crederete ma la previdenza sociale statunitense ha messo in Rete una copia del suo intero manuale operativo imbottita di informazioni utili a loro ma anche incredibilmente preziose per gli ingegneri sociali. Contiene abbreviazioni, termini gergali e istruzioni per chiedere quel che si vuole, come descritto in questa storia.

Volete saperne di più sulla previdenza sociale americana? Basta cercare su Google oppure digitare sul browser il seguente indirizzo: http://policy.ssa.gov/poms.nsf/A meno che non abbiano già letto queste pagine e tolto il manuale quando le leggerete voi, troverete istruzioni online, comprese anche indicazioni dettagliate sui dati che un impiegato può rivelare alla polizia. In pratica, a tutti gli ingegneri sociali che sono in grado di convincerlo di essere agenti.

UNA BANALE TELEFONATA

Uno dei principali problemi degli attaccanti è riuscire a far sembrare ***ragionevoli*** le loro richieste: qualcosa che suoni identi-

co alle solite richieste fatte di continuo alla vittima, qualcosa che non la sbilanci molto. E come per tante cose nella vita, fare una richiesta logica può essere difficile un giorno ma elementare il giorno dopo.

La telefonata a Mary H

Data/ora: lunedì **23** novembre, ore 7:49
Luogo: Mauersby & Storch Accounting, New York

Per tanti la contabilità significa solo maneggiare numeri e conti, e la considerano divertente quanto una trapanazione a un canino. Per fortuna non la pensano tutti così. Mary Harris, per esempio, era molto presa dal suo lavoro di ragioniera, motivo per cui era uno dei dipendenti più ligi dello studio.

Quel particolare lunedì arrivò presto al lavoro per iniziare in anticipo una lunga giornata, e rimase stupita sentendo subito squillare il telefono a quell'ora. Rispose, dando il suo nome.

"Salve, sono Peter Sheppard della Arbuckle Support, la ditta che vi fornisce l'assistenza tecnica. Durante il fine settimana abbiamo ricevuto un paio di lamentele di persone che avevano problemi con i vostri computer. Pensavo di risolvere prima che arrivassero tutti. Ha qualche problema con la macchina o con la connessione alla Rete?"

Lei gli rispose che non lo sapeva ancora, poi accese il computer. Durante la fase di awio Peter le spiegò cosa voleva fare. "Vorrei eseguire un paio di controlli con lei. Sul mio schermo posso vedere quali tasti batte e vorrei essere sicuro che vadano correttamente in Rete. Quindi ogni volta che preme un tasto deve dirmi qual è. Così controllo se compare corretto qui da me. Va bene?"

Sconvolta da visioni da incubo del computer guasto e di una giornata frustante nell'impossibilità di lavorare, Mary fu ben felice dell'aiuto. Dopo qualche secondo rispose: "Sono sulla schermata del log-in e adesso batto la ID. M... A.. . R... Y... D."

"Fin qui è perfetto. Lo vedo. Adesso batta la password ma non me la dica. Non deve rivelarla a nessuno, nemmeno ai tecnici. Io qui vedo solo asterischi, perché la sua password è protetta." Niente di tutto ciò era vero, ma aveva un senso per Mary. Poi lui aggiunse: "Mi awerta quando il computer è pronto".

Quando Mary lo avvertì lui le fece aprire due applicazioni, e lei riferì che si erano aperte bene, felice che tutto sembrasse normale. Peter disse: "Sono lieto di averla aiutata a risolvere i problemi con il computer. A proposito, abbiamo appena installato un aggiornamento che permette di cambiare le password.

È disposta a concedermi un paio di minuti per vedere se funziona?".

Lei era tanto grata per l'aiuto che disse subito di sì. Allora Peter le indicò passo passo come lanciare l'applicazione che consente di cambiare password, elemento standard del sistema operativo Windows 2000. "Adesso inserisca la password, però ricordi di non dirla ad alta voce," concluse.

Una volta fatto, aggiunse: "Tanto per controllare, quando le chiede la nuova password inserisca 'test 123', poi lo ribatta nello spazio della verifica e prema Invio".

L'accompagnò lungo il processo della sconnessione al server, poi la fece attendere un paio di minuti prima di ricollegarsi, stavolta con la nuova password. Funzionava che era una bellezza e Peter sembrava molto compiaciuto e le spiegò che adesso poteva tornare alla vecchia password o sceglierne una nuova, sempre avvertendola di non dirla ad alta voce.

"Bene, Mary, non abbiamo trovato problemi, fantastico. Senta, se per caso succede qualcosa basta che chiami alla Arbuckle. Di solito io sono ai progetti speciali ma qui chiunque può darle una mano." Lei lo ringraziò e lui salutò.

La versione di Peter

Molti ex compagni di scuola sapevano che Peter era diventato un maghetto del computer in grado di scovare informazioni utili precluse agli altri. Quando Alice Conrad gli chiese un favore, all'inizio lui si schermì. Perché? Visto che quando le aveva chiesto di uscire lei aveva rifiutato.

Però quel diniego non parve sorprenderla minimamente, anzi, Alice disse che tanto non lo riteneva capace di farlo. Era una sfida, perché naturalmente lui sapeva di esserne in grado. E così accettò.

Ad Alice avevano offerto un contratto di consulenza per una ditta di marketing, però le condizioni non le sembravano entusiasmanti. Prima di chiedere un trattamento migliore voleva sapere com'erano i contratti degli altri consulenti.

Sentiamo la versione di Peter.

Ad Alice non lo dissi però io mi eccito quando mi chiedono una cosa che credono non sia in grado di fare e invece io so già che è una passeggiata. Be', stavolta non del tutto, ci sarebbe voluto un po' di tempo. Però era fattibile.

Le avrei fatto capire il significato della parola "sveglio".

Poco dopo le sette e mezza del lunedì mattina chiamai la sede della ditta di marketing dicendo alla segretaria che ero dello stu-

dio che gestiva i loro piani pensione e dovevo parlare con la contabilità. Aveva visto se erano già arrivati? E lei: "Credo che Mary sia in ufficio da qualche minuto. Gliela cerco".

Quando Mary rispose le rifilai la storiella dei problemi alla rete interna pensata per spaventarla a morte, così mi avrebbe aiutato più volentieri. Appena l'ebbi convinta a cambiare la password mi collegai al sistema con la stessa password temporanea che le avevo detto di usare, test **123.**

Qui entra in ballo il mago. Installai un programmino che mi consentiva l'accesso al sistema informatico della ditta ogni volta che mi pareva, con una mia password segreta. Una volta finito con Mary, cancellai le tracce in modo che nessuno potesse capire che ero stato nel sistema. Banale. Dopo aver elevato i miei privilegi di sistema, riuscii a scaricare un programma gratuito, *clearlogs*, trovato su www.ntsecurity.nu, un sito web relativo alla sicurezza.

Era ora di mettersi al lavoro. Cercai tutti i documenti con la parola "contratto" nel nome e li scaricai, poi dopo qualche altra ricerca trovai la miniera d'oro, la cartella con tutti i pagamenti dei consulenti.

Adesso Alice poteva verificare i contratti e vedere quanto pagavano gli altri consulenti. Che lo facesse lei il lavoro di gambe. Io avevo eseguito quel che mi aveva chiesto.

Dai dischi in cui li avevo riversati stampai alcuni file per mostrarle la prova, poi mi feci invitare a cena da lei. Dovreste vedere la faccia che fece mentre sfogliava il fascio di documenti dicendo: "Impossibile, impossibile".

Non mi ero portato dietro i dischetti. Erano l'esca. Doveva venire da me se li voleva, nella speranza che mi dimostrasse tutta la sua gratitudine per il favore che le avevo appena fatto.

Analizziamo l'attacco

La telefonata di Peter alla ditta di marketing è la forma più elementare di ingegneria sociale, un banale tentativo che richiedeva una minima preparazione e ha funzionato al primo colpo, in pochi minuti.

Ciliegina sulla torta, Mary, la vittima, non aveva motivo di sospettare un trucco e di fare rapporto.

L'attacco ha funzionato perché Peter ha usato tre tattiche tipiche dell'ingegneria sociale. Intanto, ha ottenuto la collaborazione di Mary spaventandola, facendole credere che il suo computer poteva essere inutilizzabile. Poi se l'è presa comoda facendole aprire un paio di applicazioni per verificare che fosse tutto a posto, rafforzando così il rapporto reciproco, la sen-

sazione di essere alleati. Alla fine, ha ottenuto una collaborazione ulteriore per la parte cruciale del lavoro sfruttando la gratitudine della donna.

Ricordandole che non doveva dire mai a nessuno la sua password, nemmeno a lui, l'ha convinta in modo subdolo ma perfetto che lui era solo interessato alla sicurezza dei file aziendali, e ciò ha aumentato la convinzione di Mary che Peter fosse chi diceva di essere visto che stava proteggendo lei e lo studio.

LA RETATA DELLA POLIZIA

Immaginatevi la scena: il governo sta cercando di incastrare un certo Arturo Sanchez che distribuisce film gratis in Internet. Le case di produzione di Hollywood sostengono che sta violando i diritti d'autore, lui invece ribatte che vuole solo spingerle a riconoscere un mercato del futuro affinché inizino a rendere scaricabili in rete i nuovi titoli, aggiungendo (correttamente) che sarebbe una nuova fonte di grosse entrate che gli studios sembrano bellamente ignorare.

Mandato di perquisizione, prego

Quando rientra a casa una sera sul tardi Arturo nota le luci spente alle finestre del suo appartamento anche se ne lascia sempre accesa una quando esce.

Va a bussare alla porta di un vicino, tirandolo giù dal letto, e così scopre che in effetti la polizia ha fatto una perquisizione nel palazzo, però i vicini sono stati confinati di sotto, quindi non sanno in quale appartamento sono entrati. Si sa solo che gli agenti se ne sono andati portando via oggetti ingombranti, però erano avvolti e quindi non si capiva cos'erano. E nessuno è uscito in manette.

Arturo controlla in casa sua. La cattiva notizia è che trova un avviso della polizia di chiamare immediatamente per fissare un appuntamento per un colloquio entro tre giorni. Quella ancora peggiore è che sono scomparsi i computer.

Arturo svanisce nella notte per andare a dormire da un amico, però è roso dall'incertezza. Quanto ne sa la polizia? L'hanno finalmente incastrato, lasciandogli però la possibilità di tagliare la corda? Oppure è tutta un'altra storia, qualcosa che lui può risolvere senza cambiare città?

Prima di continuare, fermatevi a riflettere un secondo: riuscite a immaginare un modo per scoprire che cosa sa la polizia

su di voi? Presumendo che non abbiate contatti o amici in centrale o in procura, riuscite a pensare un modo per ottenere questa informazione in veste di cittadino normale? Oppure vi viene in mente qualche tecnica nota a una persona abile nell'ingegneria sociale?

Fregare la polizia

Arturo fece così: tanto per cominciare si informò sul numero di fax di una copisteria vicina.

Poi chiamò l'ufficio del procuratore distrettuale chiedendo dell'archivio, presso il quale si presentò come un detective della contea di Lake che doveva parlare con il responsabile dei mandati di perquisizione in corso.

"Sono io," rispose la donna.

"Fantastico. Perché abbiamo perquisito un sospetto ieri sera e sto cercando di trovare il mandato."

"Li schediamo secondo indirizzo."

Quando lui le diede l'indirizzo la donna parve animarsi. "**Ah, *quello*.** Lo conosco. Il Cavaliere del copyright."

"Proprio lui. Sto cercando una copia del mandato."

"Ce l'ho proprio qui."

"Fantastico. Senta, ci sto ancora lavorando e avrei una riunione tra un quarto d'ora con i federali. Purtroppo ultimamente sono tanto distratto che ho lasciato il dossier a casa e non faccio più in tempo a passare a prenderlo. Può darmi lei le copie dei documenti?"

"Certo, non c'è problema. Può passare a prenderle."

"Magnifico, magnifico. Purtroppo sono dall'altra parte della città. Non potrebbe faxarmele?"

Era un problema ma non insormontabile. "Qui agli archivi non abbiamo il fax però mi faranno usare quello al banco al piano di sotto."

Lui allora disse che avrebbe chiamato di persona per mettersi d'accordo.

L'impiegata al banco ricevimento disse che ci avrebbe pensato lei ma prima voleva sapere chi pagava. Le serviva un codice spese.

"La richiamo," disse Arturo, poi telefonò al procuratore distrettuale identificandosi come agente di polizia e chiedendo alla segretaria il codice spese dell'ufficio. Lei glielo comunicò senza esitare.

Quando Arturo richiamò al banco per dare il numero ne approfittò per manipolare ancora un pochetto la donna, chieden-

dole se poteva andare di sopra a prendere le copie dei documenti da faxare.

Coprire le tracce

Gli restavano ancora due passaggi. C'era sempre una possibilità che qualcuno sentisse puzza di bruciato, e al suo arrivo in copisteria ci fosse ad aspettarlo un paio di agenti in borghese, i quali avrebbero finto di essere impegnati in altre faccende fino a quando non veniva qualcuno a chiedere di quel fax. Attese un po', poi richiamò il banco per verificare che il fax fosse partito. Fin qui tutto bene.

Quindi telefonò a un'altra copisteria della stessa catena in città con il trucco già visto di mostrarsi contento del loro lavoro, dicendo che gli sarebbe piaciuto inviare una lettera di congratulazioni. A proposito, come si chiamava? Con questa informazione essenziale richiamò la prima copisteria chiedendo del titolare. Quando l'uomo sollevò la cornetta Arturo disse: "Salve, sono Edward del negozio 628 di Hartfield. Anna, la titolare, mi ha detto di chiamarla perché abbiamo un cliente sconvolto. Qualcuno gli ha dato il fax del negozio sbagliato. Stiamo aspettando un fax importante solo che dall'altra parte hanno il numero della vostra filiale." L'uomo promise che avrebbe cercato il documento per inviarlo immediatamente ad Hartfield.

Arturo stava già aspettando al secondo negozio quando arrivò il fax. Appena l'ebbe in mano chiamò al banco per ringraziare l'impiegata e dirle che non era necessario riportare le copie di sopra, poteva gettarle. Quindi telefonò al direttore della prima filiale per dire anche a lui che poteva gettare il fax. In questa maniera non c'erano più prove di quanto successo, nel caso che in seguito qualcuno facesse domande. Gli ingegneri sociali sanno bene che non si è mai abbastanza prudenti.

Per giunta, Arturo non doveva nemmeno pagare il primo negozio per il fax ricevuto e rispedito al secondo. E se la polizia fosse arrivata al primo lui sarebbe già stato lontano prima che arrivassero anche al secondo.

Morale della storia: i documenti dimostravano che la polizia aveva prove fondate delle attività di riproduzione cinematografica di Arturo. Era tutto quel che voleva sapere. A mezzanotte aveva già lasciato lo stato. Stava per cominciare altrove una nuova vita con una nuova identità, pronto a riawiare la sua campagna.

In realtà nessuno di noi è immune ai raggiri di un bravo ingegnere sociale. Visti i ritmi della vita quotidiana, non sempre ci concediamo il tempo di prendere una decisione mirata persino in questioni per noi importanti. Le situazioni complicate, la mancanza di tempo, lo stato emotivo o l'affaticamento mentale possono distrarci come se niente fosse. Perciò prendiamo scorciatoie mentali, decidiamo senza analizzare con pignoleria l'informazione: un processo mentale noto come "reazione automatica". È vero persino per i funzionari degli enti pubblici e per i tutori dell'ordine. Siamo tutti fatti di carne e ossa.

Analizziamo l'attacco

Il personale degli uffici dei procuratori distrettuali è in costante contatto con le forze dell'ordine: risponde, si mette d'accordo, scambia messaggi per loro. Colui che ha abbastanza coraggio da sostenere di essere un agente, un vicesceriffo o simili viene creduto sulla parola. A meno che non sia evidente che non conosce la terminologia oppure se non sembra nervoso e non commette errori grossolani o pare sincero, non gli rivolgeranno alcuna domanda. È esattamente quanto è successo poco sopra con due persone diverse.

Il necessario codice di addebito è stato ottenuto con una sola telefonata, poi Arturo ha giocato la carta simpatia con la storia della riunione tra quindici minuti con i federali e della sua distrazione. La donna era dispiaciuta per lui, e si è fatta in quattro per aiutarlo.

Poi, usando ben due copisterie, Arturo si è parato le spalle anche per il ritiro del fax. C'è una variante per rendere ancor più difficile recuperare le tracce: invece di far mandare il documento in un'altra copisteria, l'attaccante può dare quello che sembra un numero di fax ma in realtà è l'indirizzo di un servizio Internet gratuito che riceve i fax per te e li rimanda in automatico al tuo indirizzo di posta elettronica. Così l'attaccante può scaricarlo direttamente sul suo computer senza dover mostrare il volto in nessun posto dove in seguito potrebbe essere identificato. E l'indirizzo di e-mai1 e il numero di fax elettronico possono essere abbandonati a fine missione.

RIGIRARE LA FRITTATA

Il giovane Michael Parker era una di quelle persone che capiscono un po' troppo tardi che i lavori meglio pagati vanno a chi ha la laurea. Certo, aveva avuto la possibilità di andare al college locale con una borsa di studio parziale più mutuo, però significava lavorare di sera e nei fine settimana per pagare affitto,

vitto, benzina e assicurazione dell'auto. Michael, un amante delle scorciatoie, riteneva che ci fosse un'altra maniera, meno faticosa e più fruttuosa. Avendo imparato a usare il computer da quando aveva cominciato a giocarci a dieci anni, e tuttora interessato al loro funzionamento, decise di vedere se fosse in grado di "crearsi" una laurea breve in informatica.

Laureato... con lode

Poteva entrare nei sistemi informatici dell'università dello stato, trovare i dati di uno che si era laureato con buoni voti, copiarli, incollarci sopra il suo nome e aggiungerlo alla lista dei laureandi. Però, pensandoci bene, non era un metodo molto sicuro, dovevano esserci altri dati sugli studenti passati dal campus, tasse scolastiche e simili, e chissà quant'altro. Se avesse inventato soltanto gli esami e i voti avrebbe lasciato troppe voragini.

Mentre studiava il problema capì che invece poteva riuscirci controllando se esisteva per caso un suo omonimo che si era laureato in informatica in un periodo di tempo giusto. In quel caso poteva riportare il numero della previdenza sociale dell'altro Michael Parker nelle domande di impiego e semmai l'azienda avesse controllato presso l'università si sarebbe sentita rispondere che era in effetti laureato da loro. (Molti non ci avrebbero nemmeno pensato, ma per lui era ovvio che poteva mettere un numero sulla domanda e poi, una volta assunto, inserire nei moduli da nuovo assunto quello vero. Molte aziende non pensano a controllare queste discrepanze.)

Inserirsi... nei ***guai***

Come trovare un Michael Parker negli archivi dell'ateneo? Fece così: si piazzò a un **terminale** nella biblioteca principale del campus, entrò in Internet e quindi nel sito web dell'ateneo, poi telefonò in segreteria. Alla persona che rispose propinò una storia ormai familiare. "Chiamo dal centro informatico e stiamo cambiando la configurazione di rete. Vorremmo essere sicuri di non precludervi l'accesso. A che server siete collegati?"

"Cosa intende con server?"

"A quale computer vi collegate quando cercate le informazioni sugli studenti?"

La risposta, **admin.rnu.edu**, gli diede il nome del computer che conteneva i dati del corpo studentesco. Era il primo tassello del rompicapo, adesso sapeva qual era la macchina bersaglio.

Batté la URL senza ottenere risposta, come previsto c'era un fire-

wall a bloccare l'accesso. Quindi con un simpatico programma provò a collegarsi con uno dei servizi di quel computer, trovando una porta aperta con un servizio attivo in Telnet, che permette a un computer di collegarsi a un'altra macchina remota e accedervi come se fosse collegato tramite un dumb *terminal*. Gli sarebbero bastate una user ID e una password.

Chiamò ancora in segreteria, stavolta stando ben attento a parlare con una persona diversa. Quando rispose una signora, asserì nuovamente di essere del centro informatico dell'università e di star installando un nuovo sistema per gli archivi. Le chiedeva solo il favore di collegarsi al nuovo sistema ancora in modalità test per vedere se riusciva ad accedere senza problemi ai dati accademici degli studenti. Le diede l'indirizzo IP cui collegarsi e quindi la guidò lungo la trafila.

In realtà l'indirizzo IP la portò al computer della biblioteca davanti al quale era seduto Michael. Usando la stessa procedura descritta nel capitolo 8, aveva creato un simulatore di log-in, una falsa schermata in cui inserire username e password, che sembrava quella che lei era abituata a vedere quando entrava nel sistema in cerca dei dati degli studenti. "Non funziona, dice 'log-in scorretto'."

Ormai il simulatore aveva fornito usernarne e password della donna al terminale di Michael. Missione compiuta. Alla fine le disse: *"Ah,* alcuni account non sono ancora stati inseriti nella macchina. Sistemo il suo poi la richiamo". Sempre attento a non lasciare dettagli irrisolti, come devono fare tutti gli abili ingegneri sociali, si premurò di richiamarla per informarla che il sistema in fase di collaudo non funzionava ancora e, se non le procurava fastidi, l'avrebbe richiamata appena compreso il problema.

L'archivista amichevole

Adesso Michael sapeva a quale computer doveva accedere e aveva user ID e password. Ma quali comandi doveva usare per cercare le informazioni su un laureato in informatica con il nome e la data di nascita giusti? Il database degli studenti sarebbe stato di sicuro proprietario, cioè creato nel campus per le specifiche esigenze dell'università e degli archivi, e avrebbe avuto modalità specifiche per accedere alle informazioni.

Primo passo, eliminare l'ultimo ostacolo: scoprire chi poteva guidarlo attraverso i misteri della ricerca nel database studenti. Richiamò di nuovo in segreteria, sempre a una persona diversa, dicendo che era della presidenza di ingegneria e domandando come ottenere aiuto quando sorgevano problemi nell'accedere ai file accademici degli studenti.

Qualche minuto dopo si trovava al telefono con l'amministratore del database del college e tentava di battere sul tasto simpatia. "Sono Mark Sellers della segreteria. Può avere pietà di uno nuovo? Mi dispiace disturbarla ma oggi pomeriggio sono tutti in riunione e non c'è nessuno che mi possa aiutare. Ho bisogno di ricavare un elenco di tutti i laureati in informatica tra il 1990 e il 2000. Serve entro oggi e se non ce l'ho mi sa che non resto qui per molto. Vuole aiutare un ragazzo nei guai?" Aiutare la gente faceva parte del lavoro dell'amministratore del database, perciò l'interlocutore si dimostrò superpaziente quando guidò Michael passo passo nella procedura.

Alla fine Michael aveva scaricato l'intera lista di laureati in informatica di quegli anni, e nel giro di pochi minuti aveva trovato due Michael Parker, ne aveva scelto uno, ottenuto il suo numero della previdenza sociale e le altre informazioni interessanti. Era appena diventato "Michael Parker, laureato con lode in informatica nel 1998".

Analizziamo l'attacco

Questo attacco ha usato un trucco già discusso: l'attaccante ha chiesto all'amministratore del database di accompagnarlo nei vari passi di una procedura che non conosceva. Una maniera efficace di capovolgere la situazione, come chiedere a un negoziante se può aiutarti a portare alla macchina lo scatolone con gli articoli che hai appena rubato dagli scaffali.

> Certe volte chi usa il computer è ignaro delle minacce e dei punti deboli che esistono nel mondo tecnologizzato. Ha accesso alle informazioni, eppure è privo della consapevolezza precisa delle minacce alla sicurezza. Un ingegnere sociale prenderà di mira il dipendente che non recepisce bene il valore delle informazioni cercate, e quindi accetterà più facilmente la richiesta di uno sconosciuto.

PREVENIAMO GLI ATTACCHI

Simpatia, senso di colpa e intimidazione sono tre pulsanti psicologici molto usati dagli ingegneri sociali, e queste storielle vi hanno mostrato tali tattiche in azione. Ma cosa potete fare voi e la vostra azienda per evitare questo genere di attacchi?

Proteggere i dati

Alcune storie di questo capitolo evidenziano i pericoli dell'inviare un file a una persona sconosciuta, anche se è (o sembra essere) un collega, e se il documento viene inviato *internamente,* a un indirizzo e-mail o a un fax all'interno dell'organizzazione.

La politica aziendale riguardo la sicurezza dev'essere molto specifica sulle misure contro la cessione di dati sensibili a persona non nota direttamente a chi invia. Occorre stabilire procedure severe per il trasferimento dei documenti contenenti informazioni delicate. Quando la richiesta arriva da una persona che non è nota direttamente devono esserci dei passi ben precisi da seguire per la verifica, con diversi livelli di autentica a seconda della delicatezza delle informazioni.

Ecco qualche modalità da tenere presente:

- Stabilire l'autorizzazione a sapere (il che può prevedere l'autorizzazione dal detentore dell'informazione designato all'uopo).
- Mantenere un registro personale o di settore di queste transazioni.
- Preparare un elenco di persone specificamente addestrate in queste procedure e che siano abbastanza fidate per rilasciare l'autorizzazione a inviare informazioni delicate. Imponete che soltanto a costoro sia permesso inviare informazioni agli esterni al gruppo di lavoro.
- Se si riceve una richiesta di dati per iscritto (e-mail, fax o lettera) decidete ulteriori misure di sicurezza per verificare che la richiesta arrivi realmente dalla persona che sembra.

Sulle password

Tutti i dipendenti che hanno accesso a informazioni di valore, e oggi significa praticamente tutti coloro che usano un computer, devono capire che semplici iniziative come cambiare la password, anche per pochi istanti, possono causare grosse falle nella sicurezza.

Il training alla sicurezza deve affrontare il tema delle password, anche quando e come cambiarle, qual è la password accettabile e i rischi di coinvolgere altre persone nell'operazione. L'addestramento deve soprattutto far capire a tutti i dipendenti che devono sospettare di *qualsiasi* richiesta che riguarda le loro password.

In superficie sembra un messaggio semplice da trasmettere, invece non è così, perché occorre che i dipendenti capiscano be-

ne che un semplice gesto come il cambio di password può inficiare la protezione dei dati. Possiamo dire a un bambino di guardare da tutte e due le parti prima di attraversare la strada, ma finché non capirà perché è importante ci basiamo solo sulla sua cieca obbedienza. E le regole che contemplano la cieca obbedienza sono spesso ignorate o dimenticate.

Un centro per le segnalazioni

La vostra politica di sicurezza deve prevedere una persona o un gruppo designati come centro presso cui segnalare le attività sospette che sembrano tentativi di infiltrazione nella vostra organizzazione. Tutti i dipendenti devono sapere chi chiamare ogni volta che sospettano un tentativo di intrusione elettronica o fisica. Il numero di telefono presso cui fare queste denunce dev'essere sempre a portata di mano, di modo che il lavoratore non perda tempo a cercarlo nel caso in cui sospetti un attacco in corso.

Proteggere la vostra rete

I dipendenti devono capire che il nome di un server o di una rete non è un'informazione banale, anzi, può regalare all'attaccante spunti cruciali che lo aiuteranno a guadagnarsi la fiducia o a localizzare le informazioni che cerca.

Nello specifico, le persone come gli amministratori di database che lavorano con il software appartengono alla categoria dei dipendenti con esperienza tecnica, quindi devono operare secondo regole speciali e severissime riguardo la verifica delle persone che chiamano per informazioni o consigli.

Il personale che fornisce qualsiasi genere di assistenza informatica dev'essere ben addestrato sul tipo di richiesta che farà scattare il campanello d'allarme, quella che suggerisce l'attacco di un ingegnere sociale.

Vale la pena di ricordare che dal punto di vista dell'amministratore di database dell'ultima storia del capitolo, chi chiamava rispondeva ai criteri di legittimità: telefonava dal campus ed era ovviamente all'interno di un sito che esigeva username e password. Ciò chiarisce ancora una volta l'importanza di procedure standardizzate per verificare l'identità di chi richiede informazioni, soprattutto in un caso come questo in cui quella persona stava chiedendo aiuto per accedere ad archivi riservati.

Ciò vale ancor di più per le università. Non è una novità che l'hacking sia il passatempo preferito di tanti studenti e che i lo-

ro dati, e anche quelli delle facoltà, siano un bersaglio appetito. Questo abuso è talmente diffuso che alcune grandi aziende stanno ritenendo i campus un ambiente ostile e creano regole di firewall per bloccare l'accesso dagli indirizzi che terminano con *.edu*.

Insomma, tutti i dati personali di qualsiasi genere devono essere considerati primi bersagli di un attacco e protetti come informazioni delicate.

Consigli per l'addestramento

Quasi tutti gli attacchi degli ingegneri sociali sono facilissimi da parare... per chi sa che cosa aspettarsi.

Dal punto di vista aziendale, necessita assolutamente una buona preparazione, ma c'è anche bisogno d'altro: tanti modi per ***ricordare*** alla gente che cosa ha appreso.

Usate finestre che si aprono quando si accende il computer, con un diverso messaggio ogni giorno, che dovranno essere progettate in modo da non chiudersi automaticamente, ma richiedano di cliccare una specie di conferma di averle lette.

Un'altra tattica che raccomando è quella di prevedere una serie di promemoria di sicurezza. Questi messaggi frequenti sono importanti: un programma di aggiornamento dev'essere senza soluzione di continuità. Però questi promemoria non devono essere uguali ogni volta nello stile. È dimostrato che sono assorbiti meglio quando variano nell'esposizione e presentano esempi diversi.

Un metodo eccellente è usare brevi richiami nella newsletter aziendale. Non dev'essere un articolo vero e proprio, anche se non sarebbe male una rubrica sulla sicurezza. Prevedete invece inserti a due o tre colonne, una specie di piccola pubblicità. In ogni numero della newsletter cercate di pubblicare un nuovo monito in maniera concisa ma che dia nell'occhio.

9.
La stangata inversa

La stangata, un film citato altrove in queste pagine (e secondo me il migliore mai girato sulle truffe) dipana la sua trama complessa fornendo tanti dettagli interessanti. La storia del colpaccio nel film disegna un quadro esatto di come i furbi di alto borgo gestiscono il "filo" o "cavo", uno dei tre tipi di truffa di solito chiamati "il giro grosso". Se volete scoprire come fa un gruppo di professionisti a organizzare un colpo per racimolare una grossa somma in una sola sera, non esiste manuale migliore.

Le truffe tradizionali, quale che sia il trucco specifico, seguono sempre uno schema. In certi casi, però, procedono in direzione opposta e allora sono chiamate la "stangata inversa", un balletto intricato in cui l'attaccante dispone le cose in modo che sia la vittima a chiamare *lui* per chiedere aiuto, oppure racconta che ci sarebbe un collega che ha fatto una richiesta a cui lui deve rispondere.

Come funziona?

Adesso ve lo spiego.

Quando la persona della strada pensa a un hacker, di solito le viene in mente l'immagine poco lusinghiera di un nerd introverso e solitario il cui miglior amico è il computer e che ha difficoltà a reggere una conversazione che non si svolga attraverso messaggi brevi. L'ingegnere sociale, che ha spesso competenze da hacker, possiede perlopiù un talento assai diverso, la capacità spiccata di sfruttare e manipolare la gente, di convincerla a dargli informazioni che riterreste impossibili.

La telefonata ad Angela

Luogo: filiale di Valley della Industria1 Federal Bank
Ora: 11:27

Angela Wisnowski rispose a una telefonata proveniente da un tale che sosteneva di essere in procinto di incassare un'eredità sostanziosa e voleva informazioni sui diversi tipi di conto, certificati di deposito o altri investimenti che lei poteva suggerirgli in quanto sicuri, ma con interessi decenti. Angela gli spiegò che c'era un'ampia scelta e che sarebbe stato meglio se fosse passato a discuterne di persona. Lui però era intenzionato a partire in vacanza appena arrivavano i soldi e al momento aveva parecchio da fare. A quel punto Angela iniziò a suggerire alcune possibilità e a dargli i dettagli sui frutti, su ciò che accade vendendo prima un'obbligazione eccetera, e intanto cercava di capire quale tipo di investimento si proponeva quell'uomo.

Stava facendo qualche progresso quando lui disse: "Oh, mi scusi ma ho un'altra chiamata in linea. A che ora possiamo finire la conversazione così prendo una decisione? A che ora smonta per pranzo?". Angela rispose per le 12:30, allora lui le garantì che avrebbe richiamato prima oppure il giorno seguente.

La telefonata a Louis

Le grandi banche utilizzano codici interni di sicurezza che cambiano quotidianamente. Quando qualcuno di una filiale ha bisogno di informazioni da un'altra sede conferma di averne diritto dimostrando di conoscere il codice del giorno. Come ulteriore garanzia, alcune grandi banche diffondono codici multipli ogni giorno. In un istituto della costa pacifica che chiamerò Industria1 Federal Bank ogni impiegato trovava al mattino sul computer una lista di cinque codici per la giornata, numerati da A a E.

Luogo: idem
Ora: 14:48 della stessa giornata.

Louis Halpburn non si scompose di fronte a una telefonata identica alle altre gestite regolarmente parecchie volte alla settimana.

"Pronto, sono Neil Webster e chiamo dalla filiale 3182 di Boston. Angela Wisnowski, per favore."

"È fuori a pranzo. Posso aiutarla?"

"Be', ha lasciato un messaggio in cui chiedeva informazioni per fax su un nostro cliente."

Il collega che chiamava sembrava molto stressato. "La persona che di solito pensa a queste cose è in malattia e ne ho qui una pila intera, qui a Boston sono quasi le quattro e dovrei uscire entro mezz'ora per andare dal dottore."

L'elencazione di tutti i motivi per cui l'altra persona doveva compiangerlo serviva ad ammorbidire la vittima. "Non so chi abbia preso la telefonata, ma il numero di fax è illeggibile. E 213-qualcosa. Com'è il resto?" domandò il sedicente Neil.

Quando Louis diede il numero intero l'altro disse: "Bene, grazie. Prima di faxarlo dovrei chiederle il codice B".

"Ma è lei che chiama," disse Louis con quel tanto di freddezza sufficiente a farsi intendere chiaramente dall'uomo di Boston.

Perfetto. È grandioso quando non cadono alla prima spinta. Se non resistono un tantino, è *troppo facile e mi annoio,* pensò il falso Neil. Invece a Louis disse: "E solo che ho un direttore con la fissa di avere le verifiche prima di mandare qualsiasi cosa. Senta, se non avete bisogno che vi faxiamo l'informazione a me va bene lo stesso. Non c'è bisogno di verifica."

"Angela torna tra una mezz'oretta. La faccio richiamare."

"Le dirò che non sono stato in grado di mandarle l'informazione entro oggi perché lei non si è voluto identificare come legittimo richiedente dandomi il codice. Se non sono in malattia, la chiamerò domani."

"Va bene."

"Il messaggio dice 'urgente'. Comunque non importa, senza verifica ho le mani legate. Le spieghi che ho cercato di inviare ma è stato lei a non darmi il codice, va bene?"

A quel punto Louis cedette, e all'altro capo del filo si sentì, perfettamente udibile, un sospiro scocciato.

"Va bene, un minuto, devo andare al computer. Che codice vuole?"

"Il B."

Louis mise in attesa, poi tornò in linea. "È 3184."

"Non è esatto."

"Sì, invece, il B è 3184."

"Non ho detto B, ho detto D."

"Accidenti. Un attimo."

Un'altra pausa mentre Louis controllava i codici.

"D è 9697."

"Giusto, 9697. Mando subito il fax. D'accordo?"

"Certo. Grazie."

La telefonata a Walter

"Industria1 Federa1 Bank. Sono Walter."

"Salve, Walter, sono Bob Grabowski dello Studio City filiale 38. Mi serve lo specimen di firma di un conto per fax." Lo specimen di firma non contiene solo la firma del cliente ma anche informazioni come il solito numero della previdenza sociale, la data di nascita, il cognome da ragazza della madre e certe volte anche il numero della patente. Comodissimo per l'ingegnere sociale.

"Certo. Il codice C?"

"In questo momento c'è un altro cassiere al mio computer, però ho appena usato il B e il D e li so a memoria. Mi chieda uno di quelli."

"Va bene. D?"

"9697."

Pochi minuti dopo Walter mandò il fax richiesto.

La telefonata a Donna Plaice

"Salve, sono il signor Anselmo."

"In che cosa posso esserle utile?"

"Quale numero verde devo chiamare quando voglio verificare se risulta già un accredito?"

"È un cliente?"

"Sì, ma non lo uso da un po' e adesso non so dove l'ho scritto."

"Il numero è **800-555-8600.**"

"Grazie."

La versione di Vince Capelli

Vince, figlio di uno sbirro di Spokane, sapeva fin da piccolo che non avrebbe passato la vita a fare lo schiavo tutto il giorno e a rischiare la pelle per una paga ridicola. Le sue due mete principali nell'esistenza erano andarsene da Spokane e lavorare per conto proprio. Le risate degli amici al liceo servivano soltanto a rafforzarlo in questo proposito. Loro trovavano ridicolo che ci tenesse tanto a mettere su un'impresa autonoma senza ancora avere idea di quale genere.

In cuor suo Vince sapeva che avevano ragione. L'unica cosa che era bravo a fare era il catcher nella squadra di baseball del liceo. Purtroppo non era abbastanza in gamba da guadagnarsi una borsa di studio al college, per non parlare del baseball professionista. Quindi quale attività poteva avviare?

Però quelli della sua compagnia non avevano compreso una cosa: qualsiasi cosa loro avessero, un nuovo serramanico, un bel paio di guanti caldi, una nuova ragazza carina, se a Vince piaceva, poco dopo diventava sua. Non la rubava né la sottraeva di nascosto, non era costretto. Colui che la possedeva gliela dava di sua spontanea volontà, poi dopo si domandava com'era potuto succedere. Persino chiedendolo a Vince non arrivavi a nulla, nemmeno lui sapeva spiegarselo. Sembrava che gli altri gli lasciassero fare quel che voleva, tutto qua.

Vince Capelli era un ingegnere sociale sin dalla più tenera età, sebbene non avesse mai sentito parlare di questa categoria.

I suoi amici smisero di ridere quando ebbero tutti in mano il diploma del liceo. Mentre gli altri si arrabattavano a cercare un lavoro in cui non dovessero chiedere "Vuoi le patatine con il panino", il papà di Vince lo spedì a colloquio con un vecchio collega che aveva lasciato la polizia per avviare un'agenzia di investigazioni private a San Francisco, e che assunse Vince intuendo il suo talento per quel lavoro.

Questo sei anni prima. Vince odiava la parte relativa ai consorti infedeli che significava ore istupidenti e scomode seduto di posta, però si sentiva sempre stimolato dagli incarichi in cui doveva trovare informazioni sui contanti per qualche avvocato che voleva capire se uno sfigato avesse abbastanza soldi da valere una causa. Questi incarichi gli fornivano molte possibilità di usare stratagemmi.

Come la volta in cui doveva controllare i conti bancari di un certo Joe Markowicz. Joe aveva tirato un colpo basso a un ex amico che adesso voleva sapere se il malandrino fosse abbastanza solvibile da riavere i soldi indietro in caso di denuncia.

Il primo passo di Vince sarebbe stato scoprire almeno uno, ma preferibilmente due, dei codici di sicurezza della banca per un dato giorno. Sembra quasi impossibile: cosa cavolo potrà mai spingere un bancario a smantellare un pezzo del suo sistema di sicurezza? Chiedetevelo: se decideste di farlo, sapreste come riuscirci?

Per le persone come Vince è un gioco da ragazzi.

La gente si fida di te se conosci i modi di dire dell'azienda. È un po' come dimostrare che appartieni al loro giro. Una specie di stretta di mano segreta.

Per un lavoro del genere non mi serviva granché. Di sicuro non era un'operazione a cuore aperto. Per cominciare mi bastava un numero di filiale. Quando chiamai la sede di Beacon Street a Buffalo, rispose un cassiere.

"Sono Tim Ackerman," dissi. Andava bene qualsiasi nome,

tanto non lo avrebbe riportato. "Qual è il numero della vostra filiale?"

"Il numero di telefono?" Che stupido. L'avevo appena fatto, no?

"Il numero di filiale."

"3182." Proprio così. Nessun "perché vuole saperlo?" o altro. Tanto non è un'informazione riservata, è scritto in tutti gli stampati che usano.

Passo due: chiamare la banca del mio bersaglio, farsi dare il nome di un dipendente e scoprire quando smontava per il pranzo. Angela. Usciva alle 12:30. Fin qui tutto bene.

Passo tre: richiamare la stessa sede quando Angela era a mangiare, dire che chiamavo dal numero tale di Boston e che Angela doveva ricevere delle informazioni per fax, prego darmi il codice del giorno. È questa la parte delicata. Se dovessi inventare un esame per essere laureato ingegnere sociale, imporrei una cosa del genere, quando la vittima diventa giustamente sospettosa e tu insisti fino a quando non le strappi le informazioni che ti servono. Non puoi farlo solo recitando un copione o mandando a mente una procedura, devi saper leggere la vittima, cogliere il suo umore, tirarla a riva come un pesce cui dai un po' di filo, poi tiri, poi molli, poi tiri. Fino a quando non è nella reticella e la getti nella barca, splat!

Insomma, presi all'amo quel tipo e ottenni i codici del giorno. Un bel passo avanti. Quasi tutte le banche si accontentano di un codice, e se fosse stato così sarei stato a cavallo, ma la Industrial Federal ne usava cinque, quindi uno su cinque era un po' tirato per i capelli. Con due avrei avuto molte più possibilità di arrivare all'ultimo atto della commedia. Adoro la parte "non ho detto B, ho detto D". Quando funziona è stupendo. E funziona quasi sempre.

Un terzo sarebbe stato ancora meglio. Una volta sono riuscito a ottenerne tre con una sola chiamata. B, C e D suonano abbastanza simili da permetterti di sostenere che si è sbagliato un'altra volta. Però devi avere al telefono un vero gonzo. Questo non lo era, pertanto mi accontentai di due.

I codici del giorno sarebbero stati la briscola per ottenere la carta firma. Io chiamo, l'altro chiede il codice C, però io ho solo B e D. Non è la fine del mondo. Devi mantenere il sangue freddo in casi del genere, sembrare sicuro del fatto tuo, tirare diritto. Me lo giocai liscio come l'olio con la scusa che un collega stava usando il mio computer, chiedimi un altro codice, ti prego.

Siamo tutti dipendenti dello stesso istituto, siamo tutti compagni, non rendiamoci la vita difficile. Speri che la vittima abbia in mente questo in un momento del genere. E lui recitò come da

copione. Accettò i codici che gli proposi, diedi la risposta esatta e lui mandò il fax con il documento.

Quasi fatta. Un'altra telefonata mi fruttò il numero verde per il servizio automatico in cui una voce legge le informazioni che richiedi. Con quel modulo in mano avevo tutti i numeri del conto corrente e il PIN, visto che la banca usava i primi cinque o gli ultimi quattro numeri del numero della previdenza sociale. Penna in mano, chiamai il numero verde e dopo qualche minuto di tentativi ebbi il saldo di tutti e quattro i conti del tizio, e per essere sicuro, anche depositi e prelievi recenti.

Tutto quello che aveva chiesto il cliente e spiccioli. Mi piace sempre dare un piccolo extra per tenere allegro il cliente. In fondo facciamo affari con chi è soddisfatto del servizio, no?

Analizziamo l'attacco

Il passaggio cruciale di questo episodio era ottenere i fondamentali codici giornalieri, e per riuscirci l'attaccante Vince ha usato parecchie tecniche diverse.

Ha cominciato con un minimo di insistenza quando Louis si è dimostrato reticente a dirgli il codice. Aveva ragione a essere sospettoso, i codici sono pensati per un utilizzo opposto. Sapeva che di regola doveva essere il telefonatore sconosciuto a fornire a *lui* il codice di sicurezza. È stato quello il momento critico per Vince, il cardine su cui si imperniava il successo dell'impresa.

Di fronte ai sospetti di Louis, Vince ha fatto ricorso alla psicologia appellandosi alla comprensione ("devo andare dal dottore") e con un po' di insistenza ("ne ho un'intera pila e sono quasi le quattro") e manipolazione ("le spieghi lei che non ha voluto darmi il codice"). Intelligentemente non ha fatto una minaccia diretta, l'ha solo ventilata: se non mi dai il codice io non mando le informazioni sul cliente di cui ha bisogno la tua collega, e domani le dirò che le avrei anche inviate ma tu non hai collaborato.

Però non siate troppo frettolosi a criticare Louis. In fondo, la persona al telefono sapeva (o almeno ***sembrava*** sapere) che la collega Angela aveva richiesto un fax, era al corrente dei codici e sapeva che erano identificati tramite lettere. A sentir lui il direttore della filiale li richiedeva per maggior sicurezza. Sembrava non ci fosse ragione di non dargli la verifica che richiedeva.

Louis non è un caso isolato. I bancari danno tutti i giorni i codici di sicurezza agli ingegneri sociali. Incredibile ma vero.

C'è una linea tracciata sulla sabbia oltre la quale un detective privato sfocia nell'illegalità. Vince era ancora nella legalità chiedendo il numero di filiale, e persino raggirando Louis perché gli

> I codici verbali di sicurezza equivalgono alle password in quanto forniscono un metodo comodo e affidabile di protezione dei dati, però i dipendenti devono essere al corrente dei trucchi usati dagli ingegneri sociali ed essere addestrati a non cedere le chiavi del regno.

fornisse i due codici del giorno. L'ha varcata quando si è fatto faxare informazioni riservate su un cliente della banca.

Ma per lui e per il suo cliente sono reati a basso rischio. Quando rubi soldi o beni qualcuno si accorge che sono spariti. Quando rubi informazioni, quasi sempre non lo nota nessuno perché le informazioni restano comunque in possesso di chi le fornisce.

POLIZIOTTI COME POLLI

Per un investigatore privato senza scrupoli o per un ingegnere sociale ci sono occasioni frequenti per cui gli sarebbe comodo conoscere il numero della patente di una persona, per esempio se volesse assumere l'identità di un altro per ottenere informazioni sui suoi conti bancari.

A meno di non rubare il portafogli oppure spiare da dietro nel momento più opportuno, dovrebbe essere quasi impossibile scoprire un numero di patente. Invece è una passeggiata per chiunque abbia anche limitate attitudini da ingegnere sociale.

Un certo ingegnere sociale, che chiamerò Eric Mantini, ricercava in continuazione dati sulle patenti e sulle targhe, ma riteneva un rischio eccessivo chiamare la Motorizzazione per ripetere lo stesso giochetto ogni volta che gli servivano queste informazioni. Si domandava perciò se c'era una maniera per semplificare la procedura.

Forse non ci aveva mai pensato nessuno prima, però Eric riuscì a escogitare il modo di ottenere le informazioni in un batter d'occhio tutte le volte che voleva. Ci riuscì approfittando di un servizio fornito dalla Motorizzazione del suo stato. Molte strutture del genere mettono a disposizione dati altrimenti riservati alle assicurazioni, agli investigatori privati e ad altri gruppi autorizzati dal parlamento per il bene dei commerci e della società nel suo complesso.

Owiamente, la Motorizzazione ha delle consegne precise sul tipo di dati da rilasciare. Le assicurazioni possono ottenere certe informazioni, ma non altre, gli investigatori privati idem ecc.

Per i tutori dell'ordine vige una regola diversa: la Motorizzazione fornirà qualsiasi dato a ogni agente che si identifichi. Nello stato in cui abitava Eric questa identificazione era un co-

dice richiedente rilasciato dalla Motorizzazione accompagnato dal numero della patente del poliziotto. Prima di dare informazioni l'impiegato verificava, raffrontando il nome del richiedente con il suo numero di patente e con un'altra informazione, di solito la data di nascita.

Eric stava per nascondersi dietro l'identità di un poliziotto.

Come c'è riuscito? Con una "stangata inversa" ai danni dei poliziotti!

*La stangata di **Eric***

Prima chiamò il servizio abbonati per farsi dare il numero di telefono della sede della Motorizzazione presso il Campidoglio dello stato. Gli diedero il 503-555-5000, ovviamente quello per il pubblico. Poi chiamò una vicina stazione dello sceriffo chiedendo dell'ufficio telescriventi presso il quale arrivano e partono le comunicazioni con le altre agenzie, con l'archivio criminale nazionale, per i mandati ecc. All'ufficio telescriventi disse che stava cercando il numero di telefono da dare agli agenti che chiamavano la Motorizzazione.

"Lei chi sarebbe?" chiese il vicesceriffo.

"Sono **Al** e stavo chiamando il 503-555-5753." Stava tirando a indovinare, ma di sicuro l'ufficio apposito della Motorizzazione avrebbe avuto lo stesso prefisso del numero per il pubblico, ed era abbastanza sicuro che anche gli altri tre numeri successivi fossero identici. Gli servivano solo gli ultimi quattro.

Un'ufficio telescriventi dello sceriffo non riceve chiamate dalla gente normale, e colui che chiamava conosceva quasi tutto il numero. Era owio che era una persona autorizzata.

"È 503-555-6127," disse il vice.

Quindi adesso Eric aveva il numero speciale riservato agli agenti che chiamavano la Motorizzazione. Ma non era ancora sufficiente. Doveva sapere quante linee avesse quell'ufficio, e il numero di ciascuna.

Il centralino

Per riuscirci, doveva accedere al centralino riservato ai tutori dell'ordine presso la Motorizzazione. Chiamò il dicastero delle telecomunicazioni dello stato sostenendo di essere della Nortel, ditta produttrice del DMS-100, uno dei centralini commerciali più diffusi, e chiese: "Può passarmi uno dei tecnici che lavorano al DMS-100?".

Quando glielo passarono, sostenne di essere del centro di as-

sistenza tecnica del Texas e spiegò che stavano creando un database centrale per aggiornare tutti i centralini con i più recenti upgrade di programma. Avrebbero fatto tutto da lontano, non c'era bisogno della presenza di tecnici di centralino, però serviva il numero di connessione per fare gli aggiornamenti direttamente dal centro assistenza.

Sembrava perfettamente plausibile, e così il tecnico diede il numero a Eric, che adesso poteva chiamare direttamente un centralino dello stato.

Per proteggersi dalle intrusioni i centralini commerciali di questo tipo sono protetti dalle password, come ogni rete informatica aziendale. Qualsiasi ingegnere sociale in gamba con un passato di phreaking sa che la Nortel fornisce un account di default per gli aggiornamenti, NTAS (che sta per Nortel Technical Assistance Support, non molto brillante). Ma la password? Eric cercò più volte di collegarsi, ogni volta con le scelte più ovvie e comuni. Inserire il nome dell'account, NTAS, non funzionò. Né "helper" e così via.

Poi provò con "update"... e fu dentro. Tipico. Una password owia e facile da indovinare è appena meglio di non avere una password.

Non fa mai male essere aggiornati nel proprio campo: Eric doveva sembrare esperto di quel centralino e di come programmarlo e saperne risolvere i problemi almeno quanto il tecnico impersonato. Una volta in grado di accedervi come utente autorizzato avrebbe controllato le linee bersaglio. Dal proprio computer cercò il centralino relativo al numero che gli avevano dato per le chiamate degli agenti, **555-6127,** e scoprì che c'erano altre 19 linee nello stesso dipartimento. Ovviamente gestivano una quantità enorme di chiamate.

Per ogni telefonata in arrivo, il centralino era programmato in modo da "cacciare" le 20 linee fino a quando avesse trovato quella libera.

Scelse il 18 e inserì il codice di trasferimento chiamata, dando il numero del suo nuovo telefonino prepagato, lo stesso usato dagli spacciatori perché costa tanto poco da poterlo gettare appena finito il lavoro.

Adesso, con il trasferimento di chiamata sulla linea 18, appena l'ufficio era abbastanza impegnato da avere già 17 chiamate in corso, la telefonata non sarebbe arrivata alla Motorizzazione bensì al cellulare di Eric, che si mise comodo ad aspettare.

Una telefonata alla Motorizzazione

Poco prima delle otto del mattino il cellulare squillò. Era la parte più gratificante. Ecco Eric, l'ingegnere sociale, che parla

con un poliziotto, uno che potrebbe venire ad arrestarlo o fare una perquisizione dietro mandato per raccogliere prove contro di lui.

E non solo una chiamata, ma una sfilza, una dopo l'altra. In un'occasione particolare a Eric capitò di essere a tavola al ristorante con gli amici e di ricevere una telefonata ogni cinque minuti. Fu costretto a trascrivere le informazioni su un tovaglioli-no di carta con una penna prestata. Ride ancora.

Parlare con un agente di polizia non turba minimamente l'ingegnere sociale, anzi, l'eccitazione suscitata dall'inganno ai danni dei poliziotti lo rendeva ancor più divertente.

Secondo Eric andò così:

"Motorizzazione. Desidera?"

"Sono il detective Andrew Cole."

"Buongiorno. Cosa posso fare per lei?"

"Mi serve un Soundex sulla patente 005602789," rispose l'altro, usando il classico termine per quando si chiede una foto, dettaglio utile quando devono arrestare una persona e vogliono sapere che faccia abbia.

"Certo, adesso cerco la scheda," disse Eric. "Detective Cole, la sua agenzia?"

"Contea di Jefferson."

Poi Eric fece le domande cruciali. "Detective, il codice richiedente? Numero della patente? Data di nascita?"

Cole diede le informazioni personali per l'identificazione, poi Eric finse di controllare, disse che le informazioni erano confermate e chiese i particolari di quanto l'agente voleva dalla Motorizzazione. Quindi fece finta di cercare mentre Cole sentiva battere sui tasti, e alla fine tornò al telefono. "Accidenti, il computer è andato di nuovo in bomba. Mi dispiace, detective, ma fa così da una settimana. Le dispiace richiamare e parlare con un altro impiegato?"

In questo modo poteva interrompere la chiamata senza suscitare sospetti per la sua incapacità a rispondere alla richiesta. Adesso aveva rubato un'identità, tutti i dettagli che poteva usare per avere le informazioni confidenziali dalla Motorizzazione.

Dopo aver risposto alle chiamate per qualche ora ottenendo decine di codici richiedente, si collegò al centralino per disattivare il trasferimento di chiamata.

Per mesi avrebbe svolto i lavori che gli venivano passati dalle irreprensibili agenzie di investigazioni private che non volevano sapere come otteneva le informazioni. Ogni volta che ne aveva bisogno telefonava al centralino, attivava il trasferimento di chiamata e raccoglieva un'altra messe di credenziali di agenti di polizia.

Analizziamo l'attacco

Riguardiamo in moviola i trucchi usati da Eric. Nel primo passaggio fortunato ha convinto un vicesceriffo dell'ufficio telescriventi a dare a uno sconosciuto un numero riservato della Motorizzazione, visto che questi l'ha identificato come agente senza chiedere verifica.

Poi qualcuno al dicastero statale delle Telecomunicazioni ha fatto altrettanto, dando per scontato che la chiamata provenisse dawero dalla fabbrica di apparati, fornendogli così il numero per collegarsi con il centralino che serviva la Motorizzazione.

Eric è riuscito ad accedervi soprattutto a causa delle deboli misure di sicurezza del fabbricante, che usava lo stesso account su tutte le macchine. Questa disattenzione ha reso semplice indovinare la password, sapendo che i tecnici dei centralini, come chiunque, scelgono quelle più semplici da ricordare.

Dopo l'accesso al centralino, Eric ha impostato il trasferimento di chiamata da una linea riservata agli agenti al proprio cellulare.

E poi, la parte più eclatante, ha ingannato una serie di agenti in modo che rivelassero i codici richiedente e anche i dati personali, per poter essere in grado di impersonarli.

Anche se per questa impresa occorreva una certa competenza tecnica, essa non sarebbe bastata senza l'aiuto di una serie di persone inconsapevoli di avere a che fare con un impostore.

Questa storia è un'altra prova dello strano fenomeno di come mai la gente non si chieda "perché proprio io?". Perché l'agente delle telescriventi ha dato l'informazione a un vicesceriffo che non conosceva (in questo caso a un *estraneo che si spacciava* per vicesceriffo) invece di consigliargli di chiedere a un collega o al suo sergente? Anche qui l'unica risposta che posso dare è che la gente pone di rado domande. Non gli viene in mente di chiedere? Non vogliono sembrare aggressivi e poco disponibili? Forse. Ulteriori spiegazioni sarebbero solo ipotetiche. Agli ingegneri sociali non interessa il motivo: interessa loro solo che questo comportamento renda elementare ottenere informazioni che altrimenti sarebbero inaccessibili.

> Se avete un centralino in azienda, che cosa farebbe la persona incaricata nel ricevere una telefonata del fornitore che vuole sapere il numero? A proposito, questa persona ha mai cambiato la password di default per il centralino? E questa password è una parola facile, reperibile nel vocabolario?

Un codice di sicurezza usato in modo adeguato aggiunge un livello prezioso di protezione. Un codice di sicurezza utilizzato in modo improprio può essere peggio di niente, perché regala l'illusione di sicurezza che in realtà non avete. A che servono i codici se i vostri dipendenti non li tengono segreti?

Qualsiasi azienda con necessità di codici di sicurezza verbali deve spiegare chiaramente ai dipendenti quando e come essere usati. Se fosse stato addestrato bene, il personaggio del primo aneddoto di questo capitolo non si sarebbe basato sull'istinto, facilmente raggirato, quando gli è stato richiesto di rivelare a uno sconosciuto un codice di sicurezza. Ha intuito che l'altro non doveva richiedergli quell'informazione date le circostanze, ma in mancanza di una chiara politica di sicurezza, e di un minimo di buon senso, ha ceduto subito.

Le procedure di sicurezza dovrebbero anche prevedere le misure da prendere nel caso in cui un collega ponga una richiesta inappropriata. Tutti i dipendenti dovrebbero essere preparati a segnalare immediatamente ogni richiesta sospetta di credenziali di autentica come il codice quotidiano o la password. Dovrebbero anche segnalare quando un controllo dell'identità del richiedente dia risposta negativa.

Come minimo il dipendente dovrebbe segnare il nome di chi chiama, il numero di telefono e l'ufficio, poi appendere. Prima di richiamare dovrebbe verificare se l'organizzazione ha davvero uno stipendiato con quel nome e se il numero corrisponde a quello segnalato nell'elenco aziendale. Quasi sempre questa semplice tattica basterà per verificare se chi chiama è dawero quello che sostiene di essere.

La verifica diventa un po' più macchinosa quando l'azienda ha un elenco su carta invece che in rete. La gente viene assunta e se ne va, cambia settore, posizione e telefono. L'elenco su carta è già datato il giorno successivo alla stampa, persino prima della distribuzione. Anche quelli in rete non sono sempre affidabili dato che gli ingegneri sociali sanno come modificarli. Se un impiegato non può verificare il numero da una fonte indipendente, dovrebbe essere addestrato a verificare in altro modo, come per esempio rivolgendosi al suo superiore.

Terza parte

Allarme intruso

10.
Entrare nella struttura

Perché è tanto facile per un estraneo assumere l'identità del dipendente di un'azienda e recitare in maniera tanto convincente da ingannare persino le persone più pignole? Perché è tanto facile raggirare individui attentissimi alle procedure di sicurezza, sospettosi delle persone che non conoscono direttamente e pronti a proteggere gli interessi dell'impresa?

Riflettete su queste domande mentre leggete le storie di questo capitolo.

IL SORVEGLIANTE IMBARAZZATO

Data/Ora: martedì 17 ottobre, ore 2:16

Luogo: Skywatcher Aviation, Inc., stabilimento di produzione alla periferia di Tucson, Arizona.

La versione del custode

Il rumore dei suoi tacchi nei corridoi semideserti dell'impianto era molto più gradevole a Leroy Greene delle ore notturne passate di fronte ai monitor in ufficio. Là dentro aveva da guardare solo gli schermi, non poteva nemmeno leggere una rivista o la Bibbia rilegata in pelle. Doveva solo stare immobile a guardare immagini in cui non si muoveva niente.

Invece, mentre si aggirava per i corridoi poteva almeno allungare le gambe e, quando si ricordava di muovere anche braccia e spalle, faceva persino un minimo di ginnastica, sebbene non fosse un grande esercizio per uno che aveva giocato nella difesa

della squadra liceale di football vincitrice del campionato cittadino. Comunque un lavoro è un lavoro.

Dopo avere svoltato verso sud-ovest si awiò lungo la galleria che dominava il chilometro di lunghezza del capannone. Al piano di sotto due individui stavano passando accanto agli elicotteri in fase di assemblaggio e sembravano prestare attenzione ad alcuni particolari. Uno strano spettacolo a quell'ora di notte. Pensò che fosse il caso di controllare.

Si awiò verso la scala che l'avrebbe portato alle spalle dei due, i quali non si accorsero del suo arrivo. "Salve. Posso vedere i vostri tesserini, prego?" disse. Leroy cercava sempre di essere delicato in momenti del genere, a intimidire bastava la sua mole.

"Salve, Leroy," disse uno dei due leggendo il nome sul tesserino di riconoscimento. "Sono Tom Stilton dell'ufficio marketing della sede di Phoenix. Sono in città per alcune riunioni e volevo far vedere al mio amico come costruiscono i più grandi elicotteri al mondo."

"Sissignore. Tesserino, prego." Leroy non poté fare a meno di notare quanto erano giovani. Il tipo del marketing sembrava fresco di liceo, l'altro, con i capelli lunghi fino alle spalle, dimostrava quindici anni.

Quello dai capelli corti cercò il documento in tasca, poi iniziò a frugarsi dappertutto. Leroy cominciò di colpo ad avere un brutto presentimento. "Accidenti, devo averlo lasciato in macchina. Vado a prenderlo, mi dia solo dieci minuti per andare al parcheggio e tornare," disse il tipo.

A quel punto Leroy era già sul chi vive. "Come ha detto che si chiama?" chiese, appuntando diligentemente la risposta, poi domandò se potevano seguirlo nell'ufficio della sorveglianza. Nell'ascensore che li portava al terzo piano Tom spiegò di essere con la Skywatcher solo da sei mesi e che sperava di non avere guai per questo.

Nella stanza degli schermi gli altri due del turno di notte si unirono a Leroy nell'interrogatorio. Stilton diede il proprio numero di telefono e spiegò che il suo capo era Judy Underwood, di cui fornì il numero di casa. Le informazioni risultarono esatte, una volta controllate al computer. Leroy prese da parte i due colleghi per discutere sul da farsi. Nessuno voleva commettere errori, tutti e tre erano d'accordo sul chiamare il capo del tipo anche se significava svegliarla in piena notte.

Fu Leroy a telefonare, spiegando chi era e chiedendo se c'era un certo Stilton che lavorava per lei. La donna parve semiaddormentata mentre rispondeva di sì.

"Be', l'ho trovato presso la catena di montaggio alle due e mezza di notte, privo di tesserino."

La signora Underwood chiese se poteva parlargli.

Stilton andò al telefono. "Judy, mi dispiace tantissimo che ti abbiano svegliata a quest'ora. Spero che non ce l'avrai con me." Ascoltò qualche secondo, poi aggiunse: "Tanto dovevo essere qui domattina per la riunione sul nuovo comunicato stampa. A proposito, hai ricevuto la e-mai1 sul contratto Thompson? Dobbiamo parlare con Jim lunedì mattina se non vogliamo perderlo. E poi io sono a pranzo con te martedì, se ben ricordo."

Ascoltò ancora, poi salutò e appese.

Leroy ci rimase di stucco. Aveva pensato che il giovanotto gli avrebbe restituito la cornetta perché la donna gli confermasse che andava tutto bene. Si chiese se fosse il caso di richiamare, ma non riuscì a decidersi. L'aveva già scocciata in piena notte, e se avesse chiamato una seconda volta forse si sarebbe lamentata con i suoi superiori. Si disse che non valeva la pena di osare ancora.

"Allora, posso mostrare al mio amico la catena di montaggio?" chiese Stilton. "Vuole venire con noi per controllare?"

"Andate e guardate. Ma la prossima volta non si dimentichi il tesserino. E deve avvertire la sorveglianza se vuole entrare nell'impianto a quest'ora, è la regola," disse Leroy.

"Me ne ricorderò," garantì Stilton, poi i due se ne andarono.

Erano passati dieci minuti al massimo quando nell'ufficio suonò il telefono. Era la signora Underwood. "Chi era quel tale?" voleva sapere. Spiegò poi che lei gli aveva rivolto delle domande ma quello sconosciuto non faceva che parlare di un pranzo con lei anche se non sapeva nemmeno chi era.

I ragazzi della sorveglianza chiamarono l'atrio e la guardia al cancello del parcheggio, ma furono informati che i due giovanotti erano usciti da qualche minuto.

Quando rievocava quell'episodio Leroy concludeva sempre dicendo: "Santo cielo, il mio capo mi ha fatto a pezzettini. Sono fortunato a non aver perso il posto".

La versione di Joe Harper

Solo per vedere di cosa era capace, da un anno il diciassettenne Joe Harper si intrufolava nei posti, certe volte di giorno, certe volte di notte. Figlio di un musicista e di una cameriera che facevano entrambi turni di notte, Joe passava troppo tempo da solo. La sua versione dello stesso episodio chiarisce in modo istruttivo che cosa è successo.

C'è questo mio amico Kenny che è convinto di voler fare il pilota d'elicottero e mi ha chiesto se riuscivo a farlo entrare alla Skywatcher per vederne la catena di montaggio. Sa che sono so-

lito entrare nei posti, e che vado in picco d'adrenalina a infilarmi dove non dovrei stare.

Però non è facile entrare in una fabbrica o in una ditta. Bisogna pensarci bene, pianificare e fare una ricognizione sul luogo. Poi controllare la pagina web dell'azienda per cercare nomi, cariche e numeri di telefono. Leggere articoli su quotidiani e riviste. Le ricerche meticolose sono il mio marchio di fabbrica, perciò dopo posso discutere dell'argomento con chiunque come fossi un dipendente.

Da dove cominciare? Intanto cercai in Internet per sapere dove fosse la sede, così verificai che la centrale stava a Phoenix. Perfetto. Chiamai chiedendo dell'ufficio marketing, tanto ogni azienda ce l'ha, e alla signora al telefono riferii che ero della Blue Pencil Graphics e che volevo sapere se erano interessati a usare i nostri servizi e, nel caso, con chi potevo parlare. La donna mi citò un certo Tom Stilton. Quando chiesi il suo interno ribatté di non poter dare informazioni del genere, però poteva passarmelo. Trovai la segreteria con un messaggio che diceva: "Sono Tom Stilton della grafica, interno 3147, per favore lasciate un messaggio". Certo, non ti possono dire gli interni però l'amico lo mette in segreteria. Furbo. Adesso avevo nome e numero diretto.

Un'altra telefonata allo stesso ufficio. "Salve, stavo cercando Tom Stilton ma non c'è. Vorrei fare una domanda veloce al suo capo." Anche il capo era fuori, ma alla fine avevo scoperto come si chiamava. E anche lei aveva lasciato simpaticamente il numero di telefono in segreteria.

Potevo anche prevedere di passare senza problemi oltre la guardia nell'atrio, ma quando ero stato nell'impianto avevo notato un reticolato attorno al parcheggio. Un reticolato significa una guardia che ti controlla quando cerchi di entrare. E di sera prendono anche il numero di targa, perciò dovevo comprarne una vecchia al mercato dell'usato.

Intanto mi serviva il numero di telefono del gabbiotto. Attesi un po', così nel caso avessi trovato la stessa centralinista non avrebbe riconosciuto la voce. "Abbiamo un reclamo, il telefono del gabbiotto di Ridge Road segnala problemi a intermittenza. Ne hanno ancora?" Lei disse di non saperne niente ma mi avrebbe messo in collegamento.

Quando risposero: "Cancello Ridge Road, sono Ryan", io replicai: "Salve, Ryan, sono Ben. Avete problemi con i telefoni?". Era solo un guardiano mal pagato ma doveva essere ben addestrato perché chiese: "Ben chi? Come fa di cognome?". Io proseguii come se non l'avessi sentito. "Hanno segnalato un problema."

Sentii che posava la cornetta e gridava: "Ehi, Bruce, Roger,

problemi con i telefoni?", poi tornò al microfono e disse di non esserne a conoscenza.

"Quante linee avete?"

S'era dimenticato che non gli avevo più dato il mio cognome.

"Due."

"Su quale sei adesso?"

"3140."

Tombola! "Funzionano tutte e due?"

"Così pare."

"Bene. Stammi a sentire, Tom. Se avete problemi chiamate subito alle telecom. Siamo qui per esservi utili."

Decisi di andare a visitare l'impianto con il mio amico la notte successiva. Nel pomeriggio sul tardi chiamai al gabbiotto usando il nome del tipo del marketing. "Salve, sono Tom Stilton della grafica, abbiamo un problema per il quale stanno venendo due tizi nella speranza di risolverlo. Non credo che arriveranno lì prima delle due di notte. Ci siete ancora a quell'ora?"

Il guardiano fu lieto di dire che lui smontava a mezzanotte.

"Bene, lasci un biglietto per quelli del turno successivo, va bene? Quando arrivano due tizi a nome Tom Stilton fateli entrare, d'accordo?" dissi.

Sì, andava bene. Prese il mio nome, ufficio e interno e garantì che ci avrebbe pensato lui.

Arrivammo al cancello poco dopo le due, io citai il nome Stilton e a quel punto la guardia assonnata indicò la porta da cui dovevamo passare e il punto in cui parcheggiare.

Quando entrammo nel capannone trovammo un altro posto di controllo nell'atrio con il solito registro per le firme fuori orario. Dissi alla guardia che dovevo approntare una relazione entro il mattino e che questo mio amico voleva vedere l'impianto. "Va matto per gli elicotteri, vuole imparare a guidarli," spiegai. Lui mi chiese il tesserino. Io mi frugai nelle tasche, poi dissi di averlo dimenticato in macchina ma che potevo andare a prenderlo, ci impiegavo solo dieci minuti. Allora lui: "Non importa, firmi qui".

Che favola la catena di montaggio. Fino a quando non arrivò quell'armadio di Leroy.

Nell'ufficio della sorveglianza ricordai a me stesso che un estraneo sarebbe parso nervoso e spaventato. Invece io, quando le cose si mettono sul difficile, esco dai gangheri come se fossi scocciato perché non mi vogliono credere.

Appena cominciarono a dire che dovevano chiamare il mio capo, e andarono a recuperare il suo numero dal computer, io pensai che era giunto il momento di squagliarsela. Purtroppo c'era il cancello del parcheggio. Anche se fossimo usciti dal ca-

pannone loro avrebbero chiuso il cancello e saremmo rimasti in trappola.

Quando Leroy chiamò la capoufficio di Stilton e mi passò il telefono, quella iniziò a gridare chiedendo chi fossi, ma io continuai a parlare come se stessimo intrattenendo una simpatica discussione, poi riattaccai.

Quanto ci vuole a trovare qualcuno che ti dia un numero di telefono aziendale in piena notte? Pensai che avremmo avuto meno di quindici minuti per svignarcela prima che la tipa chiamasse la sorveglianza per avvisarli dell'inganno.

Uscimmo alla svelta ma senza dare nell'occhio. Come fui sollevato quando il tipo al cancello ci fece passare.

Analizziamo l'attacco

Vale la pena di notare che in questa storia gli intrusi erano adolescenti. Era solo una bravata. Però se è stato tanto facile per due ragazzini sarebbe stato ancor più semplice per dei ladri adulti, spie industriali o un gruppo di terroristi.

Come hanno fatto tre sorveglianti esperti a permettere a due intrusi di andarsene indisturbati? E non intrusi qualsiasi, ma due ragazzi tanto imberbi che qualsiasi persona assennata si sarebbe insospettita.

All'inizio Leroy era giustamente sospettoso. Ha fatto bene a portarli su in ufficio, a interrogare colui che si faceva passare per Tom Stilton e a controllare nomi e numeri di telefono. E ha fatto bene a chiamare la capoufficio.

Alla fine però è stato fregato dall'aria sicura di sé e dall'indignazione del giovanotto. Non era il comportamento che si sarebbe aspettato da parte di un ladro o di un intruso, soltanto un vero dipendente poteva comportarsi in quel modo... o almeno così riteneva lui. Leroy doveva essere addestrato a basarsi sulle identificazioni concrete, non sull'intuito.

Come mai non è stato più diffidente quando il giovane ha appeso senza porgergli la cornetta perché sentisse dalla viva voce di Judy Underwood la conferma che il ragazzo aveva un motivo valido per trovarsi nell'impianto a quell'ora?

Leroy è stato battuto da un trucco tanto smaccato da essere ovvio. Però mettetevi un attimo nei suoi panni: a stento diplomato, preoccupato per il lavoro, indeciso se poteva disturbare una dirigente per la seconda volta in piena notte. Se foste stati in lui avreste fatto la seconda telefonata?

Certo, non era l'unica ipotesi possibile. Cos'altro poteva fare la guardia?

Anche prima della telefonata poteva chiedere ai due di identi-

ficarsi con un documento. Visto che erano arrivati in auto almeno uno dei due aveva la patente. Un eventuale nome falso poteva essere smascherato immediatamente (un professionista poteva essere fornito di documenti contraffatti, ma i due pivelli non avevano preso quella precauzione). Comunque Leroy doveva esaminare le credenziali e riportare i dati. Se poi insistevano tutti e due di non avere documenti, allora doveva accompagnarli alla macchina a recuperare il tesserino che "Tom Stilton" sosteneva di aver lasciato lì.

> La gente abituata a manipolare ha di solito una personalità accattivante, è sveglia e possiede una discreta parlantina. Inoltre, gli ingegneri sociali sono abilissimi nel deviare i processi mentali degli altri affinché collaborino meglio. Credere che una persona sia invulnerabile a queste manipolazioni significa sottovalutare le capacità e il killer instinct dell'ingegnere sociale. Invece, un bravo ingegnere sociale non sottovaluta mai il suo avversario.

Dopo la telefonata, una persona della sorveglianza doveva restare con i due fino all'uscita, per accompagnarli all'auto e prendere il numero di targa. Se fosse stato abbastanza attento avrebbe notato che la targa (quella acquistata da Joe al mercato delle occasioni) aveva gli adesivi d'immatricolazione scaduti, e questo sarebbe bastato a trattenerli per ulteriori indagini.

LA PESCA NEI CASSONETTI

"Dumpster diving" è un termine che descrive il setacciamento del pattume del bersaglio in cerca di informazioni di valore. La quantità di cose che potete imparare sul soggetto in quel modo è incredibile.

Molti non si rendono conto di quanta roba gettano via a casa loro: bollette del telefono, resoconti della carta di credito, flaconi di medicinali, saldi della banca, materiali di lavoro e tanto altro.

Sul posto di lavoro i dipendenti devono sapere che c'è chi può controllare nel cestino in cerca di informazioni utili.

Quando ero al liceo andavo a fare ***trashing*** [altra espressione per "dumpster diving"] dietro la sede dell'azienda telefonica locale, spesso da solo ma ogni tanto con qualche amico che condivideva i miei interessi. Sei un provetto pescatore di cassonetti quando hai imparato qualche trucco, tipo come evitare i sacchetti provenienti dai bagni e la necessità di indossare i guanti.

La pesca nei cassonetti non è affatto divertente, però la resa è straordinaria: elenchi interni, manuali di computer, liste di di-

pendenti, stampate che insegnano come programmare i centralini ecc., ed è tutto lì alla tua mercé.

Programmavo le mie visite notturne nel periodo in cui distribuivano i nuovi manuali, perché così i bidoni erano pieni di quelli vecchi, gettati via senza discernimento. E ci andavo anche in altre nottate a caso in cerca di memo, lettere, relazioni e simili contenenti magari notizie interessanti.

Al mio arrivo cercavo subito i cartoni, li tiravo fuori e li mettevo da parte. In quel modo se qualcuno mi avesse visto, come ogni tanto capitava, potevo spiegare che un mio amico stava traslocando e io ero in cerca di scatoloni per aiutarlo a fare i bagagli. La guardia non poneva mai attenzione ai documenti che ci avevo infilato dentro per portameli via. In certi casi mi diceva di smammare, allora io mi spostavo presso un'altra sede.

Non so come funzioni adesso, ma allora era facile intuire quali erano i sacchetti dai contenuti interessanti. La spazzatura e i resti della tavola calda erano contenuti nei sacchi grossi sparsi, mentre i cestini degli uffici erano tutti in bell'ordine assieme ai sacchetti bianchi di materiale riciclabile che poi i netturbini riempivano uno per uno e legavano.

Una volta, mentre cercavo con certi amici, trovammo dei fogli stracciati a mano. Qualcuno s'era preso la briga di ridurli in tanti pezzettini comodamente gettati in un sacchetto singolo. Portammo il sacco in un fast-food, rovesciammo i frammenti sul tavolo e iniziammo a rimetterli insieme.

Eravamo tutti appassionati di puzzle, così quella fu l'occasione stimolante di risolvere un rompicapo maxi... però il premio non fu una cosa da bambini. Alla fine avevamo ricostituito l'intero elenco username e password del cruciale sistema informatico dell'azienda.

Queste battute di pesca valevano lo sforzo e il rischio? Eccome. Persino più di quel che potete credere, perché i rischi equivalgono a zero. Era vero allora ed è vero oggi: finché non commetti un'effrazione, frugare nella spazzatura altrui è legale al cento percento.

Owio, non troverete solo phreak e hacker con la testa dentro i bidoni. Anche i poliziotti di tutto il paese controllano regolarmente la spazzatura, infatti tanti delinquenti, dai padrini della mafia ai piccoli malversatori, sono stati incriminati in base a prove raccolte dal pattume. I servizi segreti, compresi i nostri, fanno ricorso da anni a questi metodi.

Sembrerà un compito troppo umile per un James Bond, chi va al cinema preferisce vederlo menare per il naso il cattivo e portarsi a letto la bella, piuttosto che ritrovarselo immerso nel pattume fino alle ginocchia. Le vere spie dimostrano meno puzza sotto il naso quando possono recuperare qualcosa di valore

tra le bucce di banana e i fondi di caffè, i giornali e le liste per la spesa. Soprattutto se non è pericoloso.

Cash in cambio di trash

Anche le grandi aziende praticano lo sport della pesca nei cassonetti. I giornali si sono divertiti un mondo nel giugno 2000 quando hanno riferito che la Oracle (il cui capo Larry Ellison è forse il più accanito avversario della Microsoft) aveva assunto un'agenzia investigativa che, purtroppo per lui, era stata presa con le mani nel sacco. Pare che i detective fossero intenzionati a frugare tra la spezzatura di una lobby sostenuta dalla Microsoft, la ACT, senza farsi scoprire. Stando ai giornalisti, una donna dell'agenzia offrì agli uomini delle pulizie sessanta dollari per consegnarle i rifiuti della ACT, ma costoro si rifiutarono. Allora tornò la sera dopo, aumentando l'offerta a cinquecento dollari per gli addetti e duecento per il capo.

Gli inservienti dissero di no a lei e di sì alla sorveglianza.

L'autorevole giornalista online Declan McCullah intitolò il suo articolo su "Wired News" *Era la Oracle a spiare la* MS. "Time" intitolò invece il servizio, riferendosi a Ellison, *Larry il guardone*.

Analizziamo l'attacco

Dopo quello che vi ho raccontato su me e sulla Oracle, vi chiederete come mai qualcuno decida di correre il rischio di rubare il pattume di qualcun altro.

Come ho detto, la risposta è che il rischio è zero e i vantaggi corposi. Va bene, forse cercare di corrompere gli addetti alle pulizie aumenta le possibilità di conseguenze legali, ma le bustarelle non sono necessarie per uno che è disposto a sporcarsi le mani.

Il cassonetto presenta notevoli vantaggi per l'ingegnere sociale. Lì dentro può trovare abbastanza informazioni per il suo assalto all'azienda bersaglio, compresi memorandum, cariche, numeri di telefono e organigrammi dei vari progetti. Il bidone può contenere gli schemi organizzativi della struttura, informazioni sulle sue attività, programmi di viaggio ecc. Tutti questi particolari possono sembrare futili per chi ci sta dentro, ma sono informazioni preziose per un esterno.

Mark Joseph Edwards, nel suo libro *Internet Security with Windows NT,* parla di "intere relazioni buttate via per qualche refuso, password scritte su foglietti, promemoria riassuntivi contenenti numeri di telefono, intere cartelle con ancora i documenti

Il vostro pattume può essere il tesoro del nemico. Non diamo molto peso ai materiali scartati nella vita privata, perciò perché dovremmo sperare che gli altri abbiano un comportamento diverso sul posto di lavoro? È solo questione di educare la forza lavoro riguardo i pericoli (gente poco scrupolosa che scava in cerca di informazioni preziose) e i punti deboli (informazioni delicate non cancellate o distrutte come si deve).

dentro, dischetti e nastri mai cancellati o distrutti, tutta roba utile per un eventuale intruso".

L'autore continua chiedendo: "E chi sono coloro che fanno le pulizie? Avete deciso che non possono entrare nella stanza dei computer, però non dimenticatevi gli altri cestini. Se un'agenzia federale ritiene necessario fare controlli sulle persone che hanno accesso ai suoi cestini e tritadocumenti, allora dovreste farlo anche voi".

IL CAPOUFFICIO UMILIATO

Nessuno ebbe nulla da ridire quando quel lunedì mattina Harlan Fortis arrivò in ufficio al dipartimento strade della contea dicendo di essere uscito di corsa di casa e di aver dimenticato il tesserino. Il custode lo vedeva entrare e uscire ogni giorno feriale da due anni, cioè da quando lavorava lì, perciò gli fece firmare un pass temporaneo da dipendente e lo lasciò entrare.

Il pandemonio scoppiò solo due giorni dopo e lo scandalo dilagò nell'intero dipartimento. Metà di coloro che lo vennero a sapere dissero che non poteva essere vero. Quanto agli altri, non sapevano se mettersi a ridere o essere dispiaciuti per il poveretto.

In fondo George Adamson era una persona gentile, il miglior caposettore che avessero mai avuto, non si meritava una cosa del genere. Sempre che fosse vera, owiamente.

I guai erano cominciati quando George aveva chiamato Harlan nel suo ufficio un venerdì sul tardi per dirgli gentilmente che da lunedì avrebbe ricoperto un altro incarico. Presso i servizi igienici. Per Harlan non era come essere licenziato, era anche peggio perché significava un'umiliazione. Non poteva fargliela passare liscia.

Quella sera si sedette in veranda a guardare il viavai dei pendolari e alla fine vide tornare a casa da scuola un giovanotto del vicinato, David, che tutti chiamavano il "War Games Kid". Lo fermò, gli offrì una bibita che aveva comprato per l'occasione e gli propose un affare: la console ultimo grido e sei giochi in cambio di una dritta sui computer e la promessa di tacere.

Quando Harlan gli illustrò il progetto, senza scendere in particolari compromettenti, David accettò, spiegandogli che cosa

doveva fare. Doveva comprare un modem, andare in ufficio, trovare un computer con un doppino del telefono libero e attaccare il modem, lasciandolo sotto la scrivania in modo che non lo notassero. Adesso veniva la parte rischiosa. Harlan doveva mettersi al computer, installare un programma di accesso remoto e avviarlo. C'era il rischio che passasse da un momento all'altro il legittimo occupante dell'ufficio o qualcuno che lo notasse alla scrivania di un altro. Mentre eseguiva materialmente l'impresa Harlan era talmente teso che faticava a leggere le istruzioni scritte dal ragazzo. Comunque arrivò in fondo, e riuscì ad andarsene dal palazzo senza farsi notare.

Piazzare la bomba

Quella sera David si fermò a cena, poi i due complici si sedettero al computer di Harlan ed entrarono nel terminale di George Adamson. Una banalità visto che George chiedeva sempre a tutti se potevano scaricargli un file o inviarlo in sua vece e non aveva mai il tempo per precauzioni come cambiare regolarmente la password. Così, dopo un po' di tempo tutti in ufficio conoscevano la sua password.

Un po' di ricerche fruttò il file Diapobudget2002.ppt, che il ragazzo scaricò nel computer di Harlan, il quale poi gli disse di andare pure a casa e di farsi vivo un paio d'ore dopo.

Quando tornò, Harlan gli chiese di ricollegarsi con il sistema informatico del dipartimento strade per rimettere il file dove l'avevano preso, cancellando la precedente versione, poi mostrò al ragazzo la console e gli disse che se fosse andato tutto bene il giorno successivo sarebbe stata sua.

Una sorpresa per George

Non immaginereste mai che una cosa noiosa come la riunione di bilancio possa risultare interessante per qualcuno, e invece la sala riunioni del consiglio di contea era gremita, piena di giornalisti, rappresentanti dei gruppi di pressione, cittadini qualsiasi e persino due troupe televisive.

In queste sedute George si sentiva sempre sulle spine. Il consiglio teneva i cordoni della borsa e se non riusciva a essere convincente nella sua presentazione gli stanziamenti per le strade sarebbero stati decurtati e tutti avrebbero iniziato a lamentarsi delle buche, dei semafori in tilt e degli incroci pericolosi, dando la colpa a lui, e l'anno venturo sarebbe stato un inferno. Ma quando quella sera annunciarono il suo intervento si sentiva fi-

ducioso. Aveva lavorato sei settimane per quella presentazione e per i grafici PowerPoint che aveva già testato su moglie, collaboratori e qualche amico stimato. Tutti erano concordi nel dire che era la migliore relazione che avesse mai preparato.

Le prime tre diapositive andarono a gonfie vele. Tanto per cambiare i consiglieri non erano distratti e lui riusciva a essere convincente nell'esposizione.

Poi tutto d'un tratto scoppiò il finimondo. La quarta immagine doveva essere la bella foto al tramonto di una nuova bretella inaugurata l'anno prima, e invece fu molto, molto imbarazzante, un'immagine tratta da una rivista tipo "Playboy". Sentì benissimo il pubblico rimanere senza fiato, mentre lui premeva fulmineo il tasto del portatile per passare all'immagine seguente.

Era anche peggiore. Stavolta non veniva lasciato nulla all'immaginazione.

Stava ancora tentando di passare a un'altra immagine quando un'anima pia staccò la spina del proiettore, mentre il presidente batteva il martelletto con forza e gridava, nel baccano, che la riunone era aggiornata.

Analizziamo *l'attacco*

Sfruttando le competenze da hacker di un adolescente, un dipendente rancoroso è riuscito ad accedere al computer del capoufficio, scaricare un'importante presentazione in PowerPoint e sostituire alcune diapositive con altre immagini imbarazzanti. Poi ha rimesso il file nel terminale del poveretto.

Grazie al modem attaccato a un computer dell'ufficio, il giovane hacker è riuscito a collegarsi da fuori. Il programma di accesso remoto era già stato installato, perciò una volta collegato avrebbe avuto accesso a tutti i file dell'intero sistema. Visto che la macchina era collegata alla rete della struttura e già conosceva username e password del capo, ha avuto la strada libera verso i suoi file.

Mettendoci anche il tempo per scansionare e inserire le immagini dalle riviste, erano bastate poche ore. Il danno risultante alla reputazione di un brav'uomo superava ogni immaginazione.

> La stragrande maggioranza dei dipendenti trasferiti o licenziati durante un ridimensionamento di personale non dà mai problemi, ma ne basta uno soltanto per fare capire troppo tardi a un'azienda quali misure doveva prendere per prevenire un disastro. L'esperienza e le statistiche hanno dimostrato con chiarezza che la massima minaccia all'impresa viene dall'*interno*. Sono loro che sanno perfettamente dove si trovano le informazioni di valore e dove colpire l'azienda per causare il maggior danno.

Nella tarda mattinata di una bella giornata d'autunno Peter Milton entrò nell'atrio della sede di Denver della Honorable Auto Parts, un grossista a livello nazionale di ricambi auto, e attese al banco mentre la giovane addetta all'accoglienza registrava un visitatore, dava istruzioni per arrivare da loro a una persona al telefono e parlava con il corriere più o meno in contemporanea.

"Come fa a fare tante cose insieme?" chiese Pete appena la ragazza trovò il tempo per lui. Lei sorrise, owiamente contenta che se ne fosse accorto. Allora lui le disse che era dell'ufficio marketing della sede di Dallas e che doveva incontrare Mike Talbot dell'ufficio vendite di Atlanta. "Dobbiamo andare da un cliente oggi pomeriggio. Lo aspetto qui nell'atrio," spiegò.

"Marketing," disse lei pensierosa, al che Peter le sorrise aspettando di sentire il seguito. "Se fossi andata all'università avrei scelto quello. Come mi piacerebbe lavorare nel marketing."

Lui le sorrise e disse: "Kaila", leggendo il nome sulla targhetta sopra il banco, "c'è una signora nella sede di Dallas che faceva la segretaria e si è fatta trasferire all'ufficio marketing. Questo tre anni fa. Adesso è vicedirettrice e guadagna due volte tanto".

Kaila aveva gli occhi lustri. Peter continuò: "Sai usare il computer?".

"Certo."

"Vuoi che dia il tuo nome per un posto da segretaria presso l'ufficio marketing?"

Lei parve raggiante. "Per quello verrei fino a Dallas."

"Ti piacerebbe Dallas. Non posso promettere nulla nell'immediato, ma vedrò che cosa posso fare."

Lei lo trovava piuttosto carino in giacca e cravatta, con quei capelli corti e in ordine che dicevano molto della sua vita lavorativa.

Peter sedette nell'atrio, aprì il portatile e iniziò a lavorare. Dopo una decina di minuti tornò al banco. "Senti, a quanto sembra Mike è in ritardo. C'è una sala riunioni dove posso sedermi a controllare la posta elettronica mentre aspetto?"

Kaila chiamò l'addetto al programma delle sale riunioni e fece in modo che Peter ne potesse usare una libera. Seguendo un'usanza tipica delle aziende della Silicon Valley (la prima a farlo dev'essere stata la Apple) alcune salette avevano il nome di un eroe dei fumetti, altre di stelle del cinema o di catene di ristoranti. A lui dissero di andare nella saletta Minnie. Kaila lo fece firmare e gli diede le indicazioni.

Localizzata la stanza, Peter si sedette, si mise comodo e attaccò il laptop al port Ethernet.

Vi siete già fatti un'idea?

Certo, l'intruso si è connesso alla Rete *oltre il firewall aziendale*.

La versione di Anthony

Potreste anche definire Anthony Lake un affarista pigro. O forse "disonesto" rende meglio l'idea.

Invece di lavorare per gli altri aveva deciso che voleva mettersi in proprio, magari con un'attività con cui poteva starsene fermo in un posto tutto il giorno senza dover correre per mezza regione. Solo che voleva un'impresa con cui poter essere sicuro di fare soldi.

Quale genere di negozio? Non ci volle molto per deciderlo. Visto che era esperto di meccanica poteva essere un negozio di ricambi auto.

E come garantirsi il successo? La risposta arrivò al volo: convincere il grossista Honorable Auto Parts a vendergli tutta la merce di cui aveva bisogno praticamente a prezzo di costo.

Chiaro che non l'avrebbero fatto di loro spontanea volontà, però Anthony sapeva come ingannare la gente, il suo amico Mickey sapeva come entrare nei computer degli altri, e così insieme escogitarono un piano astuto.

In quel giorno d'autunno riuscì a farsi passare in maniera convincente per il dipendente Peter Milton e riuscì a intrufolarsi nella sede della Honorable collegando il suo portatile alla loro rete. Fin qui tutto bene, ma era solo il primo passo. Il resto non sarebbe stato facile, soprattutto dato che si era imposto un limite di quindici minuti. Oltre quello, il rischio di essere scoperto sarebbe diventato eccessivo.

In una precedente telefonata in cui si era finto un tecnico del loro fornitore di software aveva dato il meglio di sé. "La vostra compagnia ha acquistato un piano di assistenza biennale e vi stiamo inserendo nel database per darvi notizie sull'uscita di nuove versioni aggiornate o patch di un software che utilizzate. Perciò dovete specificarmi tutte le applicazioni che usate." La risposta fu un elenco di programmi, nella quale un amico ragioniere identificò come bersaglio MAS 90, il database con la lista di rivenditori e i termini di sconto e pagamento per ciascuno.

Grazie a questa informazione chiave, usò poi un programma per identificare tutti gli host operativi sulla rete, localizzando in breve il server usato dall'ufficio contabilità. Lanciò un programma preso dall'arsenale di tools hacker del suo portatile per identificare tutti gli utenti autorizzati sul server bersaglio, poi con un altro

provò un elenco di password molto comuni, come la stessa parola "password. Quest'ultima funzionò. Niente di strano. La gente perde tutta la propria creatività quando si tratta di scegliere le parole d'ordine.

> Addestrate i vostri a non giudicare il libro soltanto dalla copertina. Solo perché una persona è ben vestita e ben tenuta non dev'essere per questo più credibile.

Erano passati solo sei minuti e aveva quasi finito. Era dentro.

Altri tre minuti per aggiungere con molta attenzione la sua impresa alla lista clienti, con indirizzo, numero di telefono e contatto, poi per il passaggio cruciale, quello che avrebbe fatto la differenza, quello che indicava che tutte le voci dovevano essergli vendute con un ricarico dell'1% rispetto al costo della Honorable.

Terminò tutto in poco meno di dieci minuti. Si fermò quel tanto da ringraziare Kaila, dicendole che aveva finito di controllare la posta. Tra l'altro aveva sentito Mike Talbot che aveva cambiato programma e stava andando direttamente alla riunione dal cliente. Però non si sarebbe dimenticato di raccomandarla per quel posto all'ufficio marketing.

Analizziamo l'attacco

L'intruso che si faceva chiamare Peter Milton ha utilizzato due tecniche di sovversione psicologica, una programmata, l'altra improvvisata al volo.

S'è vestito come un dirigente che guadagna bene, giacca e cravatta, capelli dall'ottimo taglio. Sembrano piccoli dettagli ma fanno sempre una buona impressione. L'ho scoperto senza volerlo. Quando programmavo per la GTE California, una grossa compagnia telefonica ormai defunta, ho verificato in poco tempo che se un giorno arrivavo senza il tesserino, in ordine ma casual, maglietta, pantaloni comodi e mocassini, mi fermavano sempre per farmi domande. Dov'è il suo pass, dove lavora? Un altro giorno arrivavo ancora senza tesserino ma in giacca e cravatta, molto dirigenziale, e usavo la vecchia tecnica del rimorchio, mischiandomi a un gruppo che entrava nel palazzo o da un'entrata riservata, chiacchierando come se fossi uno di loro. In quel modo passavo sempre e anche se le guardie notavano che ero senza documento di riconoscimento non mi fermavano perché sembravo dirigenziale ed ero in compagnia di gente che sfoggiava il pass.

Così ho intuito quanto sia prevedibile il comportamento dei sorveglianti. Come tutti noi giudicavano in base all'apparenza, un grave punto debole che gli ingegneri sociali sanno come sfruttare.

Fare entrare un estraneo in un'area dove potrà attaccare un portatile alla rete aziendale aumenta i rischi di incidente relativo alla sicurezza. E perfettamente ragionevole che un dipendente, soprattutto di altra sede, voglia controllare la posta elettronica in una saletta riunioni, ma a meno che non sia garantito come dipendente fidato o che la rete non sia segmentata in modo da impedire connessioni non autorizzate, potrebbe rivelarsi l'anello debole, permettendo ai file aziendali di essere compromessi.

La seconda leva psicologica dell'attaccante è entrata in gioco quando ha notato quanto lavorava la ragazza al banco. Gestiva più cose contemporaneamente, eppure non si irritava mai e riusciva a far sentire tutti come se stesse dedicando loro la sua attenzione incondizionata. Gli è parso il marchio di una persona interessata a farsi strada nella vita. E quando poi ha affermato di essere del settore marketing ha atteso di vedere la sua reazione in cerca di prove che indicassero la nascita di un rapporto. Sì. Per lui questo significava una persona da manipolare con la promessa di aiutarla a trovare un impiego migliore. (E chiaro, se lei avesse affermato che voleva passare alla contabilità avrebbe sostenuto di avere contatti anche lì.)

Inoltre, gli intrusi adorano un'altra arma psicologica usata in questa vicenda: creare la fiducia con un attacco a due fasi. Prima Anthony ha usato l'argomento del lavoro nel settore marketing, e ha citato il nome di un altro dipendente, fra l'altro realmente esistente, come del resto la persona di cui aveva preso in prestito il nome.

Poteva far seguire alla prima conversazione la richiesta immediata di una saletta, invece si è seduto per un po' fingendo di lavorare, in teoria in attesa del collega, un altro modo per sventare possibili sospetti perché un intruso non sta certo lì a perder tempo. Certo non ha atteso a lungo, l'ingegnere sociale sa che non deve restare sulla scena del delitto più del necessario.

Solo per la cronaca: secondo il dettato della legge mentre scrivo, Anthony non ha commesso alcun reato entrando nell'atrio. Non ha commesso alcun reato nemmeno usando il nome di un vero dipendente. Non ha commesso reati facendosi ospitare nella sala riunioni, né inserendosi nella rete aziendale in cerca del computer bersaglio.

Non ha infranto la legge fino al momento in cui si è introdotto materialmente nel sistema informatico.

SPIARE KEVIN MITNICK

Tanti anni fa, quando lavoravo in una piccola ditta, mi accorsi che ogni volta che entravo nell'ufficio condiviso con altri tre informatici che con me formavano il settore IT, uno di loro (lo chiamerò Joe) passava immediatamente a una diversa finestra sullo schermo. Mi parve subito sospetto. Quando successe due volte nello stesso giorno, mi sembrò necessario risolvere l'arcano. Che cosa gli premeva nascondermi?

Il computer di Joe fungeva da terminale per accedere ai minicomputer dell'azienda, perciò installai un software di controllo sul mini VAX per spiarlo. Era un programmino che funzionava come una telecamera puntata alle spalle, facendomi vedere esattamente ciò che vedeva lui sulla sua macchina.

Le nostre scrivanie erano vicine, perciò girai il mio monitor in modo da nasconderglielo almeno in parte, anche se avrebbe potuto verificare in qualsiasi momento che lo stavo spiando. Nessun problema: era troppo immerso nel suo lavoro per accorgersene.

Quel che vidi mi lasciò a bocca aperta. Stavo assistendo affascinato all'accesso di quel bastardo ai dati sulla mia busta paga. Controllava quanto guadagnassi!

Ero lì solo da pochi mesi e immaginai che Joe non sopportasse l'idea che prendessi più di lui.

Pochi minuti dopo notai che stava scaricando dei tools da hacker usati dai pirati meno esperti che non sanno come programmarseli da soli. Quindi era un novellino e non sapeva che in quel momento gli stava seduto accanto uno dei più navigati hacker d'America. Mi parve veramente ridicolo.

Sapeva già del mio stipendio, perciò era troppo tardi per fermarlo. Ma del resto qualsiasi persona con accesso informatico alla previdenza sociale o al fisco può controllare lo stipendio altrui. Non volevo certo tradirmi facendogli capire che l'avevo scoperto. In quei giorni la mia unica meta era non dare nell'occhio, e un bravo ingegnere sociale non pubblicizza mai le proprie capacità. È preferibile che la gente ti sottovaluti, non che ti consideri una minaccia.

Così lasciai perdere e mi divertii un sacco pensando che Joe credeva di conoscere un segreto su di me quando invece era l'inverso, ero io quello in vantaggio perché avevo compreso dove volesse arrivare.

Con il tempo scoprii che tutti e tre i miei colleghi nel gruppo IT si divertivano a guardare la busta paga di quella tal segretaria carina (nel caso dell'unica ragazza) oppure di quel bel giovanotto. E stavano tutti verificando stipendio e bonus di quanti li incuriosivano, compresa la dirigenza.

Analizziamo l'attacco

Questo aneddoto evidenzia un problema interessante. I file delle buste paga erano accessibili ai responsabili dei sistemi informatici della struttura. Quindi è solo un problema di persone, di decidere di chi fidarsi. In certi casi il personale IT non resiste alla tentazione di curiosare. E può farlo perché possiede privilegi che gli permettono di scavalcare le limitazioni all'accesso a quei file.

Una prima salvaguardia sarebbe nel verificare l'accesso ai file riservati come quelli delle buste paga. Certo, tutti coloro che possiedono i privilegi necessari possono disattivare la verifica o anche cancellare le tracce che potrebbero portare a loro, ma ogni passo in più richiede ulteriore fatica da parte del dipendente con pochi scrupoli.

PREVENIAMO GLI ATTACCHI

Frugando nel pattume o ingannando un sorvegliante o una segretaria, gli ingegneri sociali invadono il vostro spazio aziendale, ma sarete lieti di sapere che potete prendere delle misure preventive.

Protezione fuori dall'orario di lavoro

Tutti i dipendenti che arrivano in ufficio senza tesserino dovrebbero essere fermati al banco dell'atrio o passare nell'ufficio della sorveglianza per il rilascio di un pass giornaliero. L'incidente del primo episodio del capitolo poteva avere esiti ben diversi, se le guardie avessero avuto procedure standard da seguire quando incontrano una persona sprowista del tesserino.

Per aziende o aree aziendali in cui la sicurezza non è una preoccupazione primaria può anche non essere importante insistere sul fatto che tutti devono avere il tesserino di riconoscimento visibile in ogni momento. Però nelle aziende con aree delicate dovrebbe essere un'esigenza standard, applicata severamente. I dipendenti devono essere educati e motivati a bloccare le persone che non hanno il pass in bella evidenza, e i dirigenti devono imparare ad accettare senza imbarazzo di essere fermati da un sottoposto.

La politica aziendale dovrebbe spiegare ai dipendenti le sanzioni previste per coloro che dimenticano spesso il tesserino, come per esempio il rinvio a casa senza paga o una nota nel loro

fascicolo. Certe aziende applicano sanzioni sempre più severe, tra cui prima la segnalazione del problema al capoufficio e poi un richiamo formale.

Inoltre, laddove ci siano informazioni preziose da proteggere, l'azienda dovrebbe introdurre procedure per autorizzare le persone che hanno bisogno di entrare fuori orano. Una soluzione possibile: richiedere che queste disposizioni siano decise dalla sorveglianza o da un altro gruppo prefissato che identificherà di routine, con una telefonata al proprio superiore o con un altro metodo ragionevolmente sicuro, l'identità di qualsiasi dipendente che chiama per awertire di un ingresso fuori orario.

Trattare con attenzione l'immondizia

La storia della pesca nel cassonetto descriveva i potenziali abusi del pattume aziendale. Le otto chiavi della saggezza in tema immondizia.

- Classificate tutte le informazioni delicate in base al livello di riservatezza.
- Mettete in atto misure aziendali per eliminare le informazioni delicate.
- Insistete affinché tutte le informazioni delicate da buttare siano triturate, e garantite un modo sicuro per sbarazzarsi delle informazioni importanti su fogli troppo piccoli per passare nel tritadocumenti. Questi ultimi non devono essere modelli economici che producano strisce di carta tali che un attaccante deciso provvisto di sufficiente pazienza potrà ricostituire. Invece, devono essere le cosiddette “cross-shedders" o comunque macchine capaci di ridurre la carta in una poltiglia inutilizzabile.
- Prima di buttarli accertatevi che siano inutilizzabili o completamente *cancellati* i supporti informatici come dischetti, Zip, CD e DVD usati per conservare i dati, nastri rimuovibili, vecchi hard disk e altri supporti del genere. Ricordatevi che la cancellazione di un file *non* lo elimina in senso stretto, può essere ancora recuperato, come hanno imparato con grande vergogna i dirigenti della Enron e altri. Gettare nel bidone un qualsiasi supporto informatico è un invito a nozze per il locale pescatore di cassonetti. (Vedi il *Vademecum* per le specifiche linee guida su come sbarazzarsi di macchine e supporti.)
- Mantenete un adeguato livello di controllo sulla selezione degli addetti alle pulizie, se necessario controllandone anche il passato.

- Ricordate periodicamente ai dipendenti di riflettere sulla natura dei materiali che buttano.
- Chiudete a chiave i cassonetti.
- Usate bidoni separati per i materiali delicati e mettetevi d'accordo affinché siano eliminati da una compagnia seria specializzata in questa attività.

Dive addio ai dipendenti

Si è già parlato in queste pagine della necessità di procedure ferree quando se ne va un dipendente con accesso a informazioni riservate, password, numeri dial-in eccetera. Le vostre procedure di sicurezza devono fornire un modo per risalire a chi è autorizzato ai vari sistemi. Potrà essere duro impedire a un ingegnere sociale determinato di superare le barriere di sicurezza, ma almeno non rendetelo facile a un ex dipendente.

Un altro passo spesso trascurato: quando se ne va un dipendente che era autorizzato a recuperare i nastri di back-up dall'archivio, dev'esserci una procedura scritta per notificare immediatamente alla ditta di stoccaggio di cancellare il nome dall'elenco autorizzati.

Il *Vademecum* fornisce informazioni dettagliate su questo argomento fondamentale, ma sarà utile elencare fin da subito alcune misure chiave da mettere in pratica, come evidenziato dalle storie appena esposte:

- Un elenco completo e dettagliato dei passi da intraprendere quando se ne va un dipendente, con speciale riguardo per chi aveva accesso a dati delicati.
- Una politica di cessazione *immediata* dell'accesso del dipendente ai computer, preferibilmente ancor prima che esca dall'edificio.
- Una procedura per recuperare il suo tesserino di riconoscimento e anche le chiavi e gli strumenti di accesso elettronico.
- Richiedete alle guardie di farsi dare un documento con foto prima di ammettere un dipendente senza il tesserino e di controllare il nome sull'elenco per verificare che faccia ancora parte dell'organigramma aziendale.

Altri passaggi sembreranno eccessivi o troppo costosi per certe aziende, ma sono adatti per altre. Tra le varie misure più severe di sicurezza abbiamo:

- Tesserini elettronici e scanner all'entrata. Ogni dipendente dovrà far passare il tesserino attraverso lo scanner per l'im-

mediata verifica elettronica del diritto a entrare nell'edificio. (Ricordate che le guardie devono essere preparate ai "rimorchi", cioè ai non autorizzati che si intrufolano in scia a un legittimo dipendente.)

- Richiedere che tutti gli impiegati dello stesso gruppo di lavoro cambino password quando uno se ne va (soprattutto se è stato licenziato). Vi sembra eccessivo? Molti anni dopo il mio breve intermezzo alla General Telephone ho saputo che quelli della sorveglianza della Pacific Bell si sono "scompisciati dalle risate" sapendo della mia assunzione alla General. Però va detto, a onore loro, che la General non appena ha scoperto, dopo avermi licenziato, di aver avuto un temibile hacker tra i suoi ranghi, ha imposto immediatamente il cambio delle password **in** *tutta l'azienda!*

Anche se non volete trasformare la vostra struttura in un carcere, avete bisogno di difendervi dal dipendente licenziato ieri e che oggi sta tornando intenzionato a far danni.

Non dimenticate nessuno

Le politiche di sicurezza hanno la tendenza a trascurare i livelli infimi, le persone, come i centralinisti, che non gestiscono informazioni delicate. Abbiamo già visto che invece sono comodi bersagli per un attaccante, e la storia dell'infiltrazione dal grossista di ricambi auto ne è l'ennesimo esempio: una persona gentile vestita come un professionista che sostiene di essere un dipendente di un'altra sede dell'azienda potrebbe anche non essere quel che sembra. Gli addetti all'accoglienza devono essere ben addestrati a chiedere gentilmente un tesserino aziendale quando è il caso, e il training non sarà diretto solo a loro, ma anche a tutti coloro che gli danno il cambio al banco d'ingresso durante la pausa pranzo o caffè.

La politica per i visitatori da fuori dovrebbe esigere la presentazione di un documento con foto e la registrazione dei dati. Non è difficile ottenere documenti falsi, ma almeno questa richiesta rende la finzione un tantino più ardua per i potenziali intrusi.

In certe aziende è sensato seguire una politica che impone ai visitatori di essere accompagnati dall'atrio e da una riunione all'altra. La procedura dovrebbe prevedere che la scorta spieghi, quando accompagna il visitatore al suo primo appuntamento, se la persona è entrata nell'edificio in veste di dipendente. Perché è importante? Perché, come abbiamo visto prima, un attaccante potrebbe spacciarsi in un modo con la prima persona che in-

contra e in un altro con le successive. È troppo facile presentarsi nell'atrio, convincere l'addetto al banco che ha un appuntamento con, che so, un progettista... poi incontrarsi con quest'ultimo al quale dirà di essere di una ditta che vorrebbe vendere alla sua azienda... e quindi, dopo questo primo incontro, essere libero di scorazzare nel palazzo.

Prima di far entrare un presunto dipendente di altra sede, bisogna verificare che sia dawero un collega. Gli addetti al banco e le guardie devono essere al corrente dei metodi usati dagli attaccanti per fingersi dipendenti in modo da accedere alla sede aziendale.

E come proteggersi contro gli intrusi che riescono a infilarsi nel palazzo e attaccare il laptop in una porta di rete oltre il firewall aziendale? Data la tecnologia odierna, è un problema. Le salette riunioni, le aule di aggiornamento e simili non dovrebbero lasciare incustodite le porte di rete ma proteggere anche quelle con firewall e router. Però la miglior tutela sarebbe l'uso di un metodo sicuro per autenticare ogni utente che si connette alla rete.

Rendete sicura la IT!

Un consiglio a chi ha orecchie per sentire: nella vostra azienda ogni persona del settore IT sa o può sapere in pochi secondi quanto guadagnate, quanto si porta a casa l'amministratore e chi usa il jet aziendale per andare a sciare.

È persino possibile che in certe ditte la contabilità o il settore IT si aumentino lo stipendio, effettuino pagamenti a un fornitore falso, cancellino le note di demerito ecc. Certe volte è solo la paura di essere beccati a garantire la loro onestà... Poi un giorno arriva una persona la cui avidità o disonestà innata la spingono a ignorare il rischio o a prendere quel che ritiene di poter arraffare senza problemi.

Naturalmente esistono delle soluzioni. I file delicati possono essere protetti imponendo i giusti controlli all'accesso in modo che solo le persone autorizzate possano aprirli. Alcuni sistemi operativi possono essere configurati in modo da conservare un registro di certe attività, come per esempio le persone che cercano di accedere a un file protetto, che abbiano successo o no.

Se la vostra azienda ha afferrato il problema e ha applicato i giusti controlli all'accesso per proteggere i dati importanti, be', state facendo grossi passi in avanti verso la direzione giusta.

11.
Fondere tecnologia e ingegneria sociale

Un ingegnere sociale sfrutta la propria capacità di manipolare le persone in modo che lo aiutino ad arrivare al suo scopo, ma spesso per il successo pieno ha bisogno di una notevole competenza tecnica e di tanta abilità con i sistemi informatici e i sistemi telefonici.

Ecco una selezione di classici raggiri in cui la tecnologia gioca un ruolo importante.

Quali sono le installazioni più sicure che vi vengono in mente, le più protette contro le intrusioni, che siano di natura fisica, elettronica o telecomunicativa? Fort Knox? Certo. La Casa Bianca? Owio. Le installazioni della difesa aerea del Nord America, il NORAD, sepolte sotto una montagna? Come no?

E che ne dite delle carceri e delle prigioni federali? Devono essere tra i posti più sicuri del paese, vero? È raro che i detenuti scappino, e anche quando succede li beccano subito. Verrebbe da pensare che un carcere federale sia invulnerabile agli attacchi degli ingegneri sociali. Vi sbagliate, non esiste un posto a prova di bomba, da nessuna parte.

Qualche anno fa un paio di dritti (truffatori professionisti) incorsero in un problema: avevano sottratto una grossa somma a un magistrato. Avevano da anni grane con la legge, ma stavolta entrarono in ballo le autorità federali che, infatti, pizzicarono uno dei due, Charles Gondorff, e lo rinchiusero in un carcere presso San Diego. Il giudice federale ne autorizzò la detenzione in quanto pericoloso per la comunità e passibile di fuga.

Il suo compare Johnny Hooker sapeva che a Charlie serviva

un buon avvocato. Ma dove trovare i soldi? Come per tutti i malviventi, i loro soldi finivano sempre in bei vestiti, auto di lusso e donnine. Johnny non aveva un centesimo da parte.

Il denaro per un buon legale doveva venire da un'altra stangata, però Johnny non poteva farcela da solo. Era sempre stato Charlie Gondorff il cervello dei loro piani, però Johnny non osava andare a trovarlo in galera per chiedergli il da farsi, soprattutto considerato che i federali sapevano che la truffa coinvolgeva due persone e non vedevano l'ora di mettere le mani sul compare. Inoltre, solo i familiari potevano andare in visita, e questo avrebbe significato dover contraffare un documento. Presentare un falso documento d'identità in un carcere federale non sembrava un'idea brillante.

No, doveva contattare Charlie in un altro modo.

Non sarebbe stato facile. Nessun detenuto di qualsiasi galera è autorizzato a ricevere telefonate. Accanto a ogni telefono dei centri federali di detenzione è affisso un cartello che dice più o meno: "Si avverte l'utente che tutte le conversazioni su questo apparecchio sono controllate e che l'utilizzo del telefono significa assenso al monitoraggio". Avere degli agenti che ascoltano la telefonata mentre commetti un reato significa allungare ulteriormente la "vacanza" a spese del governo.

Però Johnny sapeva che certe telefonate non erano sottoposte a controllo, per esempio quelle tra un detenuto e il suo legale, protette dalla Costituzione in quanto comunicazioni cliente-difensore. Anzi, la struttura in cui era prigioniero Gondorff aveva alcune linee dirette con l'ufficio del difensore pubblico federale. Appena sollevavi una di quelle cornette entravi in comunicazione con il telefono corrispondente presso quella struttura. Le aziende telefoniche chiamano "Direct Connect" questo servizio tipo linea rossa. Le autorità ignare danno per scontato che sia un servizio sicuro e invulnerabile alle intrusioni, visto che le telefonate in uscita vanno solo verso i difensori d'ufficio, mentre non possono arrivare chiamate. Anche se riusciste a ottenere quel numero, i telefoni sono programmati nel centralino in modo da "deny terminate", una goffa definizione tecnica per indicare la non autorizzazione alle telefonate in arrivo.

Poiché ogni persona scaltra anche solo minimamente è versata nell'arte dell'inganno, Johnny era sicuro che doveva esserci una soluzione. Dall'interno Charlie aveva già provato a sollevare uno di quei telefoni per dire: "Sono Tom, del centro riparazioni dell'azienda telefonica. Stiamo facendo un test su questa linea e abbiamo bisogno che digitate il 9, e poi 00". Il 9 dava accesso alle linee verso l'esterno, e lo 00 all'operatore interurbane. Non aveva funzionato, la persona che aveva risposto presso l'ufficio federale conosceva quel trucco.

Invece, Johnny se la cavò meglio e scoprì in breve che c'erano dieci palazzine nel centro di detenzione, ciascuna con una linea diretta con l'ufficio del difensore pubblico. C'era qualche ostacolo da superare, ma in quanto ingegnere sociale riuscì ad appianarli tutti. In quale unità si trovava Charlie? Qual era il numero di telefono per i servizi "direct connect" di quella palazzina? E come far pervenire un messaggio a Gondorff senza essere intercettato dai secondini?

Quello che potrebbe sembrare impossibile alla gente normale, per esempio come ottenere i numeri di telefono segreti delle istituzioni federali, per l'artista della truffa consiste spesso solo in qualche telefonata. Dopo un paio di notti agitate passate a riflettere su un piano, un mattino Johnny si svegliò con la risposta chiarissima in mente e orchestrata in cinque passaggi.

Primo, scoprire i numeri delle dieci linee dirette con l'ufficio del difensore pubblico.

Poi farli reimpostare tutti, in modo che permettessero le chiamate in arrivo.

Scoprire in quale edificio era detenuto Gondorff.

Dunque scoprire il numero telefonico di quell'unità.

E alla fine mettersi d'accordo con il complice su quando doveva aspettarsi la telefonata senza che i federali sospettassero alcunché.

Un gioco da ragazzi, pensò.

Chiamare la **Bell**...

Johnny iniziò chiamando la sede centrale della compagnia telefonica sostenendo di essere della Genera1 Service Administration, l'agenzia incaricata degli acquisti e servizi per le strutture federali, e spiegando di essere alle prese con un ordine per servizi addizionali e di avere bisogno delle informazioni necessarie per fatturare i servizi di "direct connect" già in funzione, compresi i numeri funzionanti e i costi mensili presso il centro di detenzione di San Diego. La signora al telefono fu lieta di dargli una mano.

Tanto per essere sicuro Johnny provò a fare il numero di una di quelle linee, sentendosi rispondere dal classico messaggio registrato: "Questa linea è stata scollegata o non è più in servizio", ben sapendo invece che era programmata per bloccare le chiamate in arrivo, come previsto.

Grazie alla sua ampia esperienza in procedure telefoniche sapeva di doversi mettere in contatto con un ufficio denominato Centro autorizzazioni memoria recenti cambiamenti [il Remac, Recent Change Memory Authorization Center] (mi domando

sempre chi inventi questi nomi!). Intanto cominciò chiamando l'ufficio imprese dell'azienda telefonica dicendo di essere delle riparazioni e di aver bisogno del numero del Centro autorizzazioni dell'area con il dato prefisso, corrispondente a tutte le linee del carcere. Era una richiesta normale, un'informazione classica per i tecnici che sono fuori e hanno bisogno di assistenza, quindi l'impiegato non ebbe la minima esitazione a fornirgli il numero.

Poi Johnny chiamò il Centro, diede un numero falso e disse anche a loro di essere delle riparazioni, convincendo l'impiegata al telefono ad andare su uno dei numeri che si era fatto rilasciare dall'ufficio imprese poche chiamate prima. Quando la donna fu pronta Johnny le chiese: "Questo numero è impostato su deny terminate?".

"Certo."

"Bene, questo spiega perché il cliente non può ricevere! Senta, può farmi un piacere? Deve cambiare il codice o rimuovere il deny terminate." Ci fu un momento di pausa mentre lei controllava su un altro computer per verificare che ci fosse un ordine di servizio che autorizzava il cambiamento. Alla fine l'impiegata annotò: "Questo numero ***dovrebbe*** essere limitato solo alle telefonate in uscita. Non esiste un ordine di servizio per il cambiamento".

"Certo, è un errore. Dovevamo mandare l'ordine ieri, ma la responsabile che gestisce l'abbonato ha smontato prima perché stava male e si è dimenticata di passare il lavoro ad altri. Quindi ovviamente adesso il cliente è imbufalito."

Dopo una pausa carica di tensione, in cui rifletté sulla richiesta fuori dall'ordinario e contraria alle procedure, l'impiegata acconsentì. Johnny la sentì digitare per apportare il cambiamento. E pochi secondi dopo era fatta.

Aveva rotto il ghiaccio, stabilendo una specie di rapporto con lei. Intuendo la disponibilità della donna, Johnny non esitò a premere sull'acceleratore dicendo: "Ha qualche altro minuto da dedicarmi?".

"Sì. Di cos'ha bisogno?"

"Ho parecchie altre linee dello stesso cliente, tutte con lo stesso problema. Le leggo i numeri così può verificare che non siano impostate su deny terminate, va bene?"

Pochi minuti dopo tutte e dieci le linee erano "sistemate" in modo da accettare chiamate.

Trovare Gondorff

Adesso bisognava scoprire in quale unità era detenuto Charlie, un'informazione che quanti dirigono le prigioni preferisco-

no tenere riservata. Anche qui Johnny doveva basarsi sulle sue capacità di ingegnere sociale.

Per cominciare, chiamò un carcere federale di un'altra città, Miami, ma poteva andare bene una qualsiasi, dicendo che chiamava dal centro di detenzione di New York e chiedendo di parlare con qualcuno che lavorava al Sentry del Bureau of Prisons, il sistema informatico contenente le informazioni su ogni detenuto ospite di un carcere federale del paese.

Quando l'addetto arrivò al telefono Johnny passò all'accento brooklinese. "Salve, sono Thomas del centro detenzione di New York. Il nostro collegamento al Sentry ci salta di continuo. Può trovarmi un detenuto? Penso sia lì da voi." e diede nome e numero di matricola di Gondorff.

"Non è da noi, è a San Diego," rispose l'altro qualche secondo dopo.

Johnny simulò stupore. "San Diego! Doveva essere trasferito una settimana fa su un volo federale! Stiamo parlando dello stesso tizio? Data di nascita?"

"3/12/60," lesse l'altro sul suo schermo.

"Sì, è lui. In che unità lo tengono?"

"10 nord." L'addetto rispose tutto contento, anche se non c'era alcun motivo valido per cui un agente carcerario di New York avesse bisogno di quelle precisazioni.

Adesso Johnny aveva i telefoni impostati in modo da ricevere chiamate e sapeva in quale unità era rinchiuso Gondorff. Prossimo passo, scoprire il numero di telefono dell'unità 10 nord.

Questo fu più complesso. Johnny compose un numero. Sapeva che non avrebbe squillato, perciò nessuno si sarebbe accorto che stava suonando. Così rimase a leggere una guida sulle metropoli europee mentre ascoltava il tu-tu insistente, fino a quando qualcuno sollevò la cornetta. Il detenuto all'altro capo del filo stava evidentemente cercando il proprio difensore d'ufficio, ma Johnny era preparato alla risposta giusta, quindi disse: "Ufficio difensore pubblico".

Quando l'altro chiese del suo awocato gli rispose: "Vedo se è libero. Da quale unità chiama?". Prese l'appunto, mise in attesa e tornò dopo qualche minuto spiegando che il legale era in tribunale, quindi doveva chiamare più tardi, e appese.

Perse buona parte della mattinata ma poteva andar peggio. Al quarto tentativo parlò con l'unità 10 nord. Adesso aveva anche il numero della linea diretta con l'unità di Gondorff.

Sincronizziamo gli orologi

A questo punto doveva far pervenire a Charlie un messaggio

su quando sollevare la cornetta che collegava i detenuti con il difensore pubblico. Fu più facile di quel che si immagina.

Chiamò il carcere impostando una voce dall'aria ufficiale e identificandosi come un dipendente che voleva essere passato all'unità 10 nord. La chiamata fu trasferita, e quando rispose la guardia carceraria dell'unità incriminata Johnny la fece abboccare usando la denominazione tecnica dell'ufficio che gestisce i nuovi detenuti e quelli che vengono rilasciati. "Sono Tyson dell'R&D [Receive & Discharge] e vorrei parlare con il detenuto Gondorff. Abbiamo qui delle cose sue che dobbiamo spedire e ci serve l'indirizzo. Può chiamarmelo al telefono?"

Johnny sentì il secondino che gridava in sottofondo, e dopo pochi minuti febbrili udì una voce familiare all'altro capo del filo.

Disse subito: "Non aprire bocca fino a quando non ho finito". E spiegò a Charlie che doveva far finta di mandare un pacco a qualcuno, poi aggiunse: "Se ce la fai ad andare al telefono del difensore pubblico all'una non rispondere. Se invece non puoi, dimmi l'ora cui pensi di esserci". Gondorff non rispose. Allora Johnny concluse: "Bene, fatti trovare lì all'una in punto. Ti chiamo io. Solleva la cornetta. Se per caso inizia a squillare nell'ufficio del difensore pubblico tu attacca ogni venti secondi e continua così fino a quando non mi senti".

All'una Gondorff sollevò la cornetta, e trovò Johnny in attesa. Si concessero una conversazione allegra e senza fretta, la prima di una serie di chiamate simili per progettare la truffa necessaria a racimolare i soldi per le spese legali di Gondorff, il tutto al sicuro da orecchie federali.

Analizziamo l'attacco

Questo episodio offre un primo esempio di come un ingegnere sociale riesca a far succedere cose apparentemente impossibili fregando più persone, ogni volta con un'azione che di per sé sembra poco rilevante. In realtà, ogni passo fornisce un tassello del puzzle dell'intera truffa.

La prima dipendente dell'azienda telefonica era convinta di comunicare informazioni a un responsabile della contabilità federale.

La successiva impiegata sapeva perfettamente che non doveva cambiare il tipo di servizio telefonico senza un ordine di servizio ma ha aiutato lo stesso quella persona tanto gentile, permettendogli di chiamare tutte le dieci linee del carcere direttamente connesse con l'ufficio del difensore pubblico.

Quanto al tipo del carcere di Miami la richiesta di dare una mano a un collega di un altro centro federale con un problema al computer sembrava perfettamente ragionevole. E anche se

non pareva esserci un motivo valido per chiedere qual era l'unità giusta, perché non accontentarlo?

E la guardia alla 10 nord che pensava che fosse una chiamata interna e ufficiale? Era una richiesta ragionevole, quindi ha fatto arrivare il detenuto Gondorff al telefono. Roba da poco.

Una serie di episodi ben programmati che ha fruttato una stangata intera.

LO SCARICAMENTO VELOCE

Dieci anni dopo essersi laureato in legge Ned Racine vedeva i compagni di corso abitare in belle ville con il prato davanti, frequentare circoli esclusivi, giocare a golf una o due volte alla settimana mentre lui ancora trattava cause da poco per gente che non aveva mai i soldi per saldargli la parcella. La gelosia può essere una pessima compagna. Un giorno Ned ne ebbe abbastanza.

L'unico cliente decente che aveva era uno studio contabile piccolo ma attivo, specializzato in fusioni e acquisizioni. Non chiamava Ned da molto, abbastanza da fargli capire che erano impegnati in una trattativa che, una volta annunciata sui giornali, avrebbe influenzato le quotazioni di qualche azienda. Forse azioni di secondo piano, ma in un certo senso era ancora meglio: un piccolo balzo poteva rappresentare comunque un bel guadagno in un investimento come si deve. Se solo avesse potuto accedere ai loro archivi per sapere a che cosa stavano lavorando...

Conosceva un tale che a sua volta ne conosceva un altro, al corrente di metodi non esattamente ortodossi. Costui ascoltò il piano, si illuminò tutto e accettò di dargli una mano. Per una parcella più bassa della solita, in cambio di una percentuale nel colpo in Borsa di Ned, gli diede istruzioni sul da farsi e anche un simpatico apparecchietto molto utile, appena uscito sul mercato.

Per alcuni giorni di fila, Ned tenne d'occhio il parcheggio della palazzina per uffici in cui lo studio aveva la sua sede poco pretenziosa. Quasi tutti se ne andavano tra le cinque e mezza e le sei. Alle sette il parcheggio era deserto. Gli addetti alle pulizie arrivavano alle sette e mezza. Perfetto.

La sera dopo, pochi minuti prima delle otto, Ned parcheggiò dall'altra parte della strada. Come previsto il parcheggio era vuoto, eccezion fatta per il furgone delle pulizie. Accostando l'orecchio alla porta sentì l'aspirapolvere in funzione. Bussò forte, e rimase lì in attesa in giacca, cravatta e valigetta in mano. Nessuna risposta, ma lui era un tipo paziente. Bussò ancora. Alla fine *arrivò* un addetto alle pulizie. "Salve, mi sono rimaste le chiavi chiuse dentro la macchina e dovrei andare alla mia scrivania," disse forte da oltre

> Le spie industriali e gli intrusi informatici possono anche entrare fisicamente nell'azienda bersaglio. Però, invece di usare il piede di porco, l'ingegnere sociale usa l'arte dell'inganno per convincere la persona dall'altra parte della porta a lasciarlo entrare.

la porta a vetri, mostrando il biglietto da visita sottratto tempo prima a un socio dello studio.

L'altro aprì, gli chiuse la porta alle spalle e poi risalì il corridoio accendendo le luci affinché Ned vedesse dove mettere i piedi. Perché non farlo? L'addetto alle pulizie si dimostrava gentile con una delle persone che gli permetteva di portare il pane a casa. O almeno così credeva.

Ned si sedette al computer di un socio, l'accese e installò l'apparecchietto datogli nella porta seriale USB, una cosina tanto piccola da poter stare su un anello eppure in grado di contenere più di 120 megabyte di dati. Quindi entrò in rete utilizzando username e password della segretaria del tipo, comodamente riportati su un post-it, e in meno di cinque minuti scaricò ogni foglio elettronico e documento archiviato nella postazione di lavoro e nella cartella rete del socio, pronto a tornare a casa.

SOLDI FACILI

Quando ho avuto a che fare per la prima volta con i computer, al liceo, ci toccava connetterci con un modem a un minicomputer centrale DEC PCP 11 sito nel centro di Los Angeles in condivisione con tutti i licei della città. Il sistema operativo di quel computer si chiamava RSTS/E ed è stato il primo su cui ho imparato a lavorare.

In quegli anni, verso il 1981, la DEC sponsorizzava una convention per chi usufruiva dei suoi prodotti, e un giorno lessi che la fiera-convention di quell'anno si sarebbe tenuta a Los Angeles. Su una popolare rivista per gli utenti di quel sistema operativo uscì l'annuncio di un nuovo prodotto per la sicurezza, il LOCK-11, promosso con un'astuta campagna pubblicitaria che diceva qualcosa tipo: "Sono le tre e mezza di notte e il vicino Johnny ha trovato il tuo numero di dial-in, 555-0336, al 336° tentativo. Lui è dentro e tu sei fuori. Procurati LOCK-11". La pubblicità ventilava essere un prodotto a prova di hacker, e che sarebbe stato presentato alla convention.

Non stavo nella pelle per la voglia di vederlo con i miei occhi. Anche Vinny, amico e compagno di scuola, mio socio di hacking per tanti anni, diventato in seguito mio testimone a carico, era interessato al nuovo prodotto della DEC, perciò mi invitò ad andare con lui alla manifestazione.

a

Contante in linea

Quando arrivammo la gente parlava solo del LOCK-11. A quanto pareva, i suoi progettisti stavano scommettendo una discreta sommetta sul fatto che i loro prodotti fossero a prova di bomba. Sembrava una sfida cui non potevo resistere.

Puntammo direttamente sullo stand del LOCK-11 dove c'erano tre tizi, gli sviluppatori del prodotto. Io li riconobbi subito e loro me. Già in tenera età avevo acquisito una discreta fama come phreaker e hacker per via del lungo servizio che il "Los Angeles Times" aveva pubblicato sul mio primo scontro giovanile con le autorità. Secondo l'articolo, ero riuscito a entrare a forza di chiacchiere in un palazzo della Pacific Telephone in piena notte per uscirne carico di manuali informatici, proprio sotto il naso della security. (Evidentemente il "Times" voleva un pezzo sensazionale e gli veniva vantaggioso pubblicare il mio nome. Essendo io ancora minorenne, quell'articolo violava l'usanza se non l'obbligo di non diffondere i nomi dei minori accusati di reati.)

Quando arrivai allo stand con Vinny, crebbe l'interesse da ambo le parti. Nella loro ottica, perché mi conoscevano come l'hacker di cui avevano letto ed erano abbastanza sconvolti nel vedermi. Nella nostra, perché tutti e tre i progettisti erano lì con un biglietto da cento dollari che spuntava dal pass della fiera. Il premio per chi fosse riuscito a battere il loro sistema sarebbero stati i trecento dollari, una bella sommetta per due ragazzini come noi. Non vedevamo l'ora di cominciare.

LOCK-11 era progettato su un principio assodato che si basava su due livelli di sicurezza. L'utente doveva avere una ID e una password valide, come sempre, ma avrebbero funzionato solo se inserite da terminali autorizzati, una tattica chiamata *"terminal-based security"*. Per battere il sistema, l'hacker doveva conoscere ID e password ma anche inserire queste informazioni dal terminale giusto. Era un metodo invalso, e gli inventori del LOCK-11 erano strasicuri che avrebbe tenuto alla larga i malintenzionati. Decidemmo di impartire loro una lezione, guadagnando nel frattempo i tre centoni.

Un tale che conoscevo, considerato un guru RSTS/E, ci aveva già preceduti allo stand. Anni prima, assieme ad altri, mi aveva sfidato a entrare nel computer di sviluppo interno della DEC, dopodiché i suoi soci mi avevano denunciato. Da allora era diventato uno stimato programmatore. Scoprimmo che poco prima del nostro arrivo aveva già tentato di battere il programma di sicurezza LOCK-11, ma senza fortuna, e questa disavventura aveva reso gli sviluppatori ancor più fiduciosi della sicurezza del loro prodotto.

Era una sfida molto semplice: se riesci a entrare vinci i soldi. Ottima mossa pubblicitaria... a meno che qualcuno non riuscisse a metterli in imbarazzo guadagnandosi quei dollari. Erano tanto sicuri del loro prodotto da avere persino il coraggio di attaccare allo stand una stampata con i numeri e le relative password di alcuni account sul sistema. E non solo quelli normali ma anche tutti quelli privilegiati.

Raccogliamo la sfida

Io e Vinny ci allontanammo per discutere della sfida, e a quel punto mi venne in mente un piano. Gironzolammo per un po' con aria innocente, tenendo d'occhio da lontano lo stand. All'ora di pranzo, quando la folla si diradò, i tre progettisti approfittarono della pausa per andare tutti a mangiare, lasciando a presidiare lo stand solo una signora, forse la moglie o la fidanzata di uno di loro. Tornammo di corsa, io distrassi la donna con chiacchiere di circostanza, tipo da quanto tempo lavorava in ditta, quali altri prodotti l'azienda aveva sul mercato ecc.

Intanto Vinny, di nascosto, s'era messo all'opera sfruttando un trucco che avevamo affinato insieme. A parte la bellezza dell'entrare di soppiatto nei computer e il mio interesse per la magia, eravamo anche interessati a imparare come scassinare le serrature. Da bambino avevo frugato tra gli scaffali di una libreria alternativa della San Fernando Valley piena di volumi sulle effrazioni, tipo come aprire le manette, creare false identità, tutte quelle cose che un bambino non dovrebbe sapere.

Al pari di me, Vinny si era esercitato nello scasso fino a diventare abbastanza in gamba con tutte le serrature reperibili dal ferramenta. Un tempo mi divertivo a fare scherzi con le serrature, per esempio individuare qualcuno che usava due serrature per maggior protezione, aprirle e scambiarle di posto, di modo che al proprietario sarebbe venuto un colpo cercando di aprire con la chiave sbagliata.

Continuai a distrarre la giovane mentre Vinny, chino dietro lo stand in modo da non essere scorto, apriva la serratura dell'armadietto contenente il mini PDP-11 e i cavi. Definirla serratura era quasi uno scherzo, era quella che i fabbri definiscono una "cialda", notoriamente facile da scassinare, persino per dilettanti abbastanza maldestri come noi.

Vinny ci mise circa un minuto per aprirla. Dentro l'armadietto trovò più o meno ciò che si aspettava, la sfilza di porte seriali per attaccare i terminali e una per il cosiddetto "terminale console", quello usato dall'operatore o amministratore di sistema per controllare gli altri computer. Vinny inserì il cavo che anda-

va dal port console a uno dei terminali a disposizione del pubblico.

Adesso questo computer era riconosciuto come quello console. Mi sedetti a quella specifica macchina ricollegata ed entrai usando una delle password spavaldamente fornite dai progettisti. Visto che il programma LOCK-11 mi identificava come connesso da un terminale autorizzato, mi permise l'accesso, ero perciò collegato con i privilegi di amministratore di sistema. Aggiunsi un patch al sistema operativo, in modo da potermi collegare come utente privilegiato da qualsiasi terminale dello stand.

Una volta installata la pezza segreta, Vinny si rimise al lavoro scollegando il cavetto e rimettendolo dove si trovava in origine, poi richiuse l'armadietto.

Quando feci una listing delle directory per vedere quali file conteneva il computer, in cerca del programma LOCK-11 e file relativi, incappai in qualcosa di sconcertante: una directory che non doveva trovarsi su quella macchina. I progettisti erano così ultrasicuri, talmente convinti dell'inviolabilità del loro programma da non essersi presi nemmeno la briga di togliere il codice sorgente del nuovo prodotto. Mi spostai al terminale adiacente per le stampate e iniziai a far uscire pezzi del source code sui fogli continui a righine verdi da computer che si usavano allora.

Vinny aveva appena finito di richiudere la serratura e mi raggiunse proprio nel momento in cui i tipi tornarono dal pranzo. Mi trovarono seduto al computer a digitare mentre la stampata continuava a sfornare. "Che combini, Kevin?" chiese uno.

"Oh, stampavo solo il vostro codice sorgente," risposi. Pensavano che stessi scherzando, ma quando guardarono la stampante videro che era davvero il codice sorgente, gelosamente custodito, del loro prodotto.

Ritenevano tuttora impossibile che fossi connesso come utente privilegiato. "Batti Control-T," ordinò uno dei tre. Obbedii. La schermata confermò quanto dicevo. Quello si diede una manata in fronte mentre Vinny diceva: "I trecento dollari, prego".

Pagarono. Noi due ci aggirammo per il resto della giornata con le banconote infilate nel pass della fiera. Tutti i presenti ne compresero il significato.

Certo, non avevamo battuto il loro software, e se il terzetto avesse imposto regole più sensate per la sfida o avesse usato una serratura davvero affidabile o avesse sorvegliato meglio

Ecco un altro esempio di persone in gamba che hanno sottovalutato il nemico. E voi? Siete tanto certi delle contromisure della vostra sicurezza aziendale da scommettere trecento dollari contro l'intrusione di un attaccante? Certe volte la strada per aggirare' un'apparecchiatura per la sicurezza non è quella che vi aspettate.

le macchine, non sarebbero stati umiliati... per giunta da due adolescenti.

Poi venni a sapere che la squadra di progettisti dovette passare dalla banca a prelevare: quelle tre banconote da cento erano tutti i soldi che avevano con sé.

IL VOCABOLARIO COME ARMA D'ATTACCO

Quando qualcuno ottiene la vostra password è in grado di invadere il vostro sistema. Quasi sempre non vi accorgete nemmeno che è successo qualcosa di spiacevole.

Un giovane attaccante, che chiamerò Ivan Peters, s'era prefissato di ottenere il source code di un nuovo gioco elettronico. Non ebbe problemi a entrare nella wide area network dell'azienda, perché un suo amico hacker aveva già compromesso un server web di quella compagnia. Dopo aver trovato un punto debole nel software privo di patch del server, il suo compare era quasi cascato dalla sedia vedendo che il sistema era stato impostato come "dual-homed host", indicando così che poteva entrare nella rete interna.

Ma quando Ivan si collegò, si trovò di fronte a un problema simile a chi entra nel Louvre per cercare la Gioconda. Senza una pianta poteva vagare per settimane intere. Quella era un'azienda globale, con centinaia di sedi e migliaia di server, e non fornivano certo l'indice dei sistemi di sviluppo o i servizi di un cicerone per arrivare al punto giusto.

Invece di usare la tecnologia per scoprire qual era il server da prendere di mira, Ivan usò una tattica classica dell'ingegnere sociale. Fece alcune telefonate basate su metodi simili a quelli descritti nelle pagine di questo libro. Prima chiamò l'assistenza tecnica IT, sostenendo di essere un dipendente con un problema di interfaccia in un prodotto che il suo gruppo stava progettando, chiedendo il numero di telefono del capo della squadra sviluppo giochi.

Poi chiamò la persona indicatagli, facendosi passare per uno della IT. "Stasera cambiamo router e vogliamo essere sicuri che la vostra squadra non perda la connessione al vostro server. Perciò dobbiamo sapere quali usate." La rete veniva aggiornata di continuo e comunque dare il nome del server non danneggiava nessuno, no? Essendo protetta da password, il solo nome non aiutava alcuno a intrufolarsi. Così quella persona rivelò il nome all'attaccante e non si premurò nemmeno di richiamare per verificare la scusa né appuntò nome e numero di telefono. Diede solo il nome dei server, ATM5 e ATM6.

L'attacco alle password

A questo punto Ivan passò al versante tecnologico per ottenere le informazioni sull'autentica. Il primo passo in quasi tutti gli attacchi tecnici sui sistemi che consentono l'accesso remoto è identificare un account con una password debole, che fornisca il punto di entrata nel sistema.

Quando un attaccante tenta di usare tools da hacker per le password di identificazione remota, l'impresa può richiedere alcune ore, restando collegati alla rete dell'azienda. E chiaro che lo si fa a proprio rischio e pericolo: più si rimane collegati maggiore è la probabilità di essere individuati.

Come primo passo Ivan doveva fare un'enumerazione per svelare i dettagli del sistema bersaglio. Anche in questo caso Internet fornisce comodi programmi all'uopo (presso http://ntsleuth.0catch.com. Il carattere prima di "catch è uno zero). Ivan trovò parecchi strumenti da hacker a disposizione del pubblico che rendevano automatico il processo di enumerazione per evitare di doverlo fare a mano, il che avrebbe comportato più tempo e maggior rischio. Sapendo che l'organizzazione cui era interessato usava soprattutto server basati su Windows, scaricò una copia di NBTEnum, una utility di enumerazione NetBIOS (un banale sistema input/output), inserì l'indirizzo IP (Internet protocol) del server ATM5 e aprì il programma. Il tool di enumerazione riuscì a identificare parecchi account sul server.

Una volta identificati gli account esistenti, lo stesso tool iniziò a scatenare un "attacco a vocabolario" contro il sistema informatico. Un "dictionary attack" è una faccenda ben nota a tanti intrusi ed esperti della sicurezza informatica, ma quasi tutti gli altri rimarranno sgomenti ad apprendere che una cosa del genere è possibile. Questo attacco mira a scoprire la password di ogni utente del sistema utilizzando parole di uso comune.

Noi siamo tutti pigri in certe cose, ma non cessa mai di stupirmi come la creatività e l'immaginazione tendano ad affievolirsi quando la gente sceglie le password. Quasi tutti vogliamo una password che protegga e sia nel contempo facile da ricordare, il che significa di solito qualcosa che ci è vicinissimo. Le nostre iniziali, il soprannome, il nome del o della consorte, la canzone, il film o la birra preferiti, tanto per fare un esempio. Il nome della strada o della città in cui abitiamo, il modello di auto che guidiamo, il villaggio vacanze cui siamo stati alle Hawaii o quel torrente prediletto con le migliori trote da pescare. Riconoscete uno schema mentale? Sono di solito nomi propri, di località o parole del vocabolario. Un "attacco a vocabolario" vaglia le parole comuni a ritmo rapidissimo, provandone ciascuna su uno o più account.

Ivan lo condusse in tre fasi. Per la prima usò una semplice lista delle 800 password più comuni, che comprende "segreto", "lavoro" e "password. Inoltre il programma permutava ogni termine con un numero suffisso o con quello del mese corrente, e questo su tutti gli account identificati. Niente da fare.

Per il tentativo seguente Ivan entrò nel motore di ricerca Google e digitò "wordlists dictionaries" trovando migliaia di siti contenenti immensi elenchi di parole in inglese e in parecchie lingue straniere. Scaricò un intero vocabolario elettronico d'inglese, arricchendolo poi con una serie di elenchi di parole trovati su Google. Scelse il sito presso www.outpost9.com/files/WordLists.html che gli permetteva di scaricare (tutto gratis) una selezione di file compresi cognomi, nomi, anche di attori, e nomenclature dalla Bibbia.

Un altro dei tanti siti che offrono liste di parole è a cura della Oxford University presso ftp://ftp.ox.ac.uk/pub/wordlists.

Altri siti offrono elenchi con i nomi dei personaggi dei fumetti, parole usate da Shakespeare, nell'*Odissea*, da Tolkien e nella serie Star *Trek*, oltre che in campo scientifico, religioso ecc. (Una ditta online vende un elenco di 4,4 milioni di parole e nomi per soli 20 dollari.) Il programma d'attacco può essere impostato per provare anche gli anagrammi delle parole del vocabolario, un altro metodo classico che gli utenti dei computer si illudono possa aumentare la sicurezza.

Più veloce di quel che credi

Una volta che Ivan decise quale wordlist usare e awiò l'attacco, il programma proseguì in pilota automatico e lui poté rivolgere la sua attenzione ad altre attività. Questa è la parte più incredibile: forse pensate che un attacco del genere abbia fatto progressi ridicoli quando l'hacker si sveglia al mattino. In realtà, a seconda della piattaforma attaccata, della configurazione di sicurezza del sistema e della connessione di rete, è possibile tentare tutte le parole del vocabolario inglese in meno di trenta minuti. Incredibile!

Mentre era in corso il tentativo, Ivan awiò un altro attacco informatico simile contro l'altro server usato dal gruppo sviluppo, l'ATM6. Venti minuti dopo il programma aveva fatto quanto molti utenti ignari amano ritenere impossibile: aveva trovato una password, rivelando che un utente aveva scelto "Frodo", uno degli hobbit del Signore degli anelli.

Con questa password in carniere fu in grado di collegarsi al server ATM6 usando l'account dell'utente.

E arrivarono notizie buone e cattive per il nostro amico. Quel-

la buona fu che l'account sfondato aveva privilegi di amministratore, essenziali per il passo successivo. Quella cattiva era che il codice sorgente del gioco non era rintracciabile da nessuna parte. Doveva essere sull'altro server, ATM5, che già sapeva essere invulnerabile all'attacco vocabolario. Tuttavia Ivan non voleva mollare, aveva ancora alcuni trucchi nel suo arsenale.

In alcuni sistemi operativi Windows e UNIX, le password cifrate (hash) sono disponibili a chiunque abbia acc'esso al computer su cui sono archiviate, per il semplice motivo che le password cifrate non possono essere decodificate e quindi non devono essere protette. Un'ipotesi sbagliata. Con un altro tool, pwdump3, anch'esso disponibile in Internet, Ivan riuscì a estrarle dall'ATM6 e a scaricarle.

Un classico file di password hashes è più o meno simile a questo:

```
Administrator:500:95E4321A38AD8D6AB75E0C8D76954A50:2E48927A0
B04F3BFB341E26F6D6E9A97:::
akasper:1110:5A8D7E9E3C3954F642C5C736306CBFEF:393CE7F90A8357
F157873D72D0490821:::
digger:1111:5D15C0D58DD216C525AD3B83FA6627C7:17AD564144308B4
2B8403D01AE256558:::
ellgan:1112:2017D4A5D8D1383EFF17365FAF1FFE89:07AEC950C22CBB9
C2C734EB89320DB13:::
tabeck:1115:9F5890B3FECCAB7EAAD3B435B51404EE:1F0115A72844721
2FC05E1D2D820B35B:::
vkantar:1116:81A6A5D035596E7DAAD3B435B51404EE:B933D36DD12258
946FCC7BD153F1CD6E:::
vwallwick:1119:25904EC665BA30F4449AF42E1054F192:15B2B7953FB6
32907455D2706A432469:::
mmcdonald:1121:A4AED098D29A3217AAD3B435B51404EE:E40670F936B7
9C2ED522F5ECA9398A27:::
kworkman:1141:C5C598AF45768635AAD3B435B51404EE:DEC8E827A1212
73EF084CDBF5FD1925C:::
```

Sulle password cifrate scaricate sul suo computer Ivan usò un altro tool che eseguiva un tipo diverso di attacco chiamato ***forza bruta,*** che prova ogni combinazione di caratteri alfanumerici e di quasi tutti i simboli speciali.

Ivan usò una utility chiamata L0phtcrack3 (pronunciata loftcrack e disponibile presso www.elcomsoft.com). Gli amministratori di sistema la usano per verificare le password deboli, gli attaccanti invece per decifrare le password. L'aspetto forza bruta di LC3 cerca le password con combinazioni di lettere, numeri e tanti simboli, compresi !@#$%^&, e tenta sistematicamente ogni combinazione possibile di più caratteri. (Sappiate però

che, se si usano caratteri non stampabili, LC3 non potrà mai scoprire la password.)

Questo programma ha una velocità quasi incredibile, che può toccare i 2,8 milioni di tentativi al secondo su una macchina con un processore di 1 Ghz. Persino a questa velocità, e se l'amministratore ha configurato il sistema operativo Windows nel modo corretto (disabilitando l'utilizzo di hashes LANMAN) trovare una password può rivelarsi un'impresa troppo lunga. Perciò l'attaccante scarica spesso gli hashes e prosegue con l'attacco sulla sua macchina o su un'altra piuttosto che restare in linea nella rete dell'azienda vittima rischiando di essere individuato.

Per Ivan non si trattò di un'attesa lunga. Qualche ora dopo, il programma gli presentò le password di tutti i componenti della squadra di sviluppatori. Però erano quelle degli utenti del server ATM6, mentre già sapeva che il codice sorgente del gioco non era lì dentro.

E adesso? Non era ancora riuscito a trovare una password di account sull'altro server. Sfruttando la sua mentalità da hacker. consapevole delle mediocri propensioni alla sicurezza dell'utente tipico, immaginò che un membro della squadra poteva avere scelto la stessa password anche per l'altra macchina.

In effetti fu quello che trovò. Uno di loro aveva usato "gamers" sia sull'ATM5 che sull'ATM6.

Adesso la porta era spalancata per la caccia di Ivan, che trovò i programmi desiderati. Una volta scovato il source code e averlo allegramente scaricato, fece un'altra mossa tipica dei cracker: cambiò la password di un account inattivo con diritti di amministratore, nel caso che in futuro volesse recuperare una versione aggiornata del programma.

Analizziamo l'attacco

In questo attacco basatosi sia sulle debolezze tecniche sia su quelle umane, Ivan ha cominciato con una telefonata pretesto per ottenere localizzazione e nomi host dei server di sviluppo contenenti le informazioni proprietarie.

Poi ha utilizzato un programma per identificare gli username validi di tutti coloro che avevano un account sul server sviluppo, quindi ha portato due successivi attacchi alle password, compreso un "attacco vocabolario" che prova le password più usate tentando tutte le parole del vocabolario inglese, certe volte arricchito da parecchi elenchi di termini contenenti nomi propri di persona, località e voci di interesse particolare.

Dato che i tool da hacker commerciali e di pubblico dominio sono a disposizione di chiunque, quale che sia lo scopo che ha

in mente, è fondamentale stare molto attenti nella protezione dei sistemi informatici aziendali e della vostra infrastruttura di rete.

La portata di questa minaccia non sarà mai sopravvalutata. Secondo la rivista "Computer World, una ricerca presso la newyorkese Oppenheimer Funds ha condotto a una scoperta sconcertante. Il vicepresidente della sicurezza della rete e riparazione danni dell'azienda ha portato un attacco alle password dei dipendenti usando un pacchetto software standard. Secondo la rivista, nel giro di *tre minuti* è riuscito a scoprire le password di tutti gli ottocento dipendenti.

> Per usare la terminologia del Monopoli, se per la vostra password usate una parola presente nel vocabolario... andate in galera direttamente senza passare dal Via. Dovete insegnare ai vostri dipendenti come scegliere le password che proteggono realmente i vostri beni.

PREVENIAMO GLI ATTACCHI

Gli attacchi degli ingegneri sociali possono diventare ancora più dannosi quando si aggiunge l'elemento tecnologia. Prevenire questo tipo di attacco significa di solito prendere iniziative sia a livello umano sia a livello tecnico.

Basta dire no

Nella prima storia di questo capitolo l'impiegata della compagnia telefonica non doveva cambiare lo status deny terminate sulle dieci linee senza un ordine di servizio che l'autorizzasse. Non basta che i dipendenti conoscano le procedure di sicurezza, devono anche capire quanto siano importanti per prevenire i danni all'azienda.

Le politiche di sicurezza devono scoraggiare le infrazioni alla procedura tramite un sistema di ricompense e punizioni. Ovviamente devono essere realistiche, non possono pretendere che i dipendenti prendano iniziative tanto gravose da essere poi ignorate. Inoltre, il programma di attenzione alla sicurezza deve convincere i dipendenti che, per quanto sia importante completare il lavoro in tempo, una scorciatoia che aggiri le misure di sicurezza potrebbe andare a detrimento di tutti.

Bisognerebbe essere altrettanto cauti quando si danno informazioni a un estraneo per telefono. Sebbene questa persona possa presentarsi in maniera convincente, nonostante il suo li-

vello all'interno della struttura, non bisogna fornire assolutamente informazioni che non siano di pubblico dominio finché non è stata verificata l'identità di chi chiama. Se questa procedura fosse stata applicata rigorosamente, il trucco dell'ingegnere sociale, citato in una storia, sarebbe andato a vuoto e il detenuto federale Gondorff non sarebbe mai riuscito a progettare una nuova truffa con il compare Johnny.

Questo punto è talmente importante da ripeterlo in tutto il libro: verificare, verificare, verificare. Ogni richiesta che non sia fatta di persona non dev'essere mai accettata senza verificare l'identità del richiedente, punto e basta.

Ripulire

Per qualsiasi azienda che non ha guardie sul posto ventiquattr'ore al giorno, il piano per cui l'attaccante entra negli uffici fuori orario presenta un grave rischio. Di solito gli addetti alle pulizie trattano con rispetto tutti coloro che sembrano dell'organico. In fondo sono persone che possono creare loro problemi o farli licenziare. Perciò essi, che siano interni o di ditte appaltatrici, devono essere istruiti sulle questioni della sorveglianza fisica.

Per pulire per terra non devi avere la laurea né saper parlare bene, e la loro preparazione classica, ammesso che esista, tratta altri problemi, come i detersivi da usare nei diversi posti. Di solito queste persone non ricevono istruzioni come: "Se qualcuno ti chiede di entrare fuori orario devi chiedere il tesserino aziendale e poi chiamare in sede da te per spiegare la situazione e domandare l'autorizzazione".

Un'organizzazione deve prevedere una situazione, come quella illustrata in questo capitolo, prima che awenga e addestrare il personale di conseguenza. Secondo la mia esperienza personale, quasi tutte se non tutte le imprese private sono molto disattente in tema di sicurezza fisica. Potete tentare di affrontare il problema dall'altro capo, scaricando l'onere sui dipendenti. Qualsiasi ditta priva di sorveglianza a tempo pieno deve far capire al proprio personale che se vogliono entrare fuori dall'orario di lavoro devono portarsi le chiavi o i tesserini di accesso e non mettere mai gli addetti alle pulizie nella condizione di decidere loro chi ammettere. Poi ricordate alla ditta che si occupa delle pulizie che il suo personale dev'essere sempre consapevole di non poter far entrare nessuno nei vostri locali in qualsiasi momento. E una regola semplice: non aprite la porta a nessuno. Nel caso, può essere inserita per iscritto nel contratto per le pulizie.

Inoltre gli inservienti devono essere consapevoli delle tecniche del "rimorchio". Devono anche sapere di non poter invitare una persona a seguirli dentro l'edificio solo perché sembra uno del posto.

Ogni tanto, diciamo tre o quattro volte l'anno, eseguite una prova di intrusione o una valutazione della vulnerabilità. Qualcuno deve presentarsi alla porta quando gli addetti alle pulizie stanno lavorando e cercare di convincerli a farlo entrare. Invece di usare un vostro dipendente potete interpellare una ditta specializzata in questa tipologia di "penetration testing".

Passaparola: proteggere le vostre password

Le organizzazioni stanno diventando sempre più attente all'applicazione di misure di sicurezza tramite la tecnologia, per esempio configurando il sistema operativo in modo da far valere una politica delle password e limitare il numero di tentativi di log-in non validi che possono essere fatti prima di escludere l'account. In effetti, di solito le piattaforme aziendali Microsoft Windows hanno questo optional incluso. Eppure questi prodotti, sapendo che i clienti sono facilmente infastiditi da questi aspetti che richiedono grattacapi in più, vengono di solito forniti con gli optional di sicurezza disattivati. È davvero venuto il momento che i produttori di software la smettano di distribuire prodotti con le voci sicurezza disattivate di default quando invece dovrebbe essere il contrario. (Sospetto che lo capiranno presto.)

La sicurezza aziendale dovrebbe imporre agli amministratori di sistema di applicare una politica di sicurezza tramite strumenti tecnologici appena possibile, per non basarsi sugli errori umani più del necessario. È lapalissiano che limitando per esempio il numero di tentativi falliti di log-in a un dato account renderete assai più difficile la vita a un attaccante.

Ogni organizzazione deve trovare quel difficile equilibrio tra una forte sicurezza e la produttività del personale, una situazione che porta alcuni dipendenti a ignorare le contromisure, a non capire quanto siano essenziali queste contromisure a salvaguardia dell'integrità di preziose informazioni aziendali.

Se le politiche dell'impresa lasciano in sospeso certi problemi i dipendenti possono adottare la via più semplice e scegliere quanto riesce più comodo e facilita loro il lavoro. Alcuni possono opporre resistenza ai cambiamenti e snobbare apertamente le buone abitudini di sicurezza. Forse avete incontrato lavoratori del genere, che osservano le regole obbligate sulla lunghezza e

complessità della password, ma poi la scrivono su un post-it appiccicato in segno di sfida allo schermo.

Una parte essenziale della protezione della vostra struttura è l'uso di password difficili da scoprire, unito a forti impostazioni di sicurezza nei macchinari.

Per un'analisi più dettagliata delle politiche raccomandate sulle password, si veda il ***Vademecum.***

12.
Attacchi al livello più basso

Come dimostrano le tante storie qui contenute, l'ingegnere sociale in gamba prende di mira di solito i lavoratori al livello inferiore della gerarchia. Può essere facile manipolare queste persone in modo che svelino informazioni apparentemente innocue che l'attaccante userà per fare un passo avanti verso il raggiungimento di informazioni più sensibili.

Un attaccante sceglie i dipendenti più umili perché di norma non sono consapevoli del valore delle specifiche informazioni o dei possibili esiti di certe azioni. Inoltre, hanno la tendenza a farsi circuire facilmente dalle più classiche tattiche dell'ingegneria sociale: una persona al telefono che finge di essere importante, un interlocutore simpatico e amichevole, uno che sembra conoscere persone della ditta note alla vittima, una richiesta urgente oppure la presunzione di potersi guadagnare una lode.

Eccovi qualche esempio di attacco al livello più basso.

L'AMICHEVOLE CUSTODE

I truffatori sperano di trovare sempre persone avide perché più passibili di cascare in un raggiro. Gli ingegneri sociali, quando prendono di mira un addetto alle pulizie o una guardia giurata, sperano di trovare una persona amichevole, paciosa e che si fida degli altri. Sono quelle che hanno più probabilità di dimostrarsi disponibili a dare una mano. E appunto quanto aveva in mente l'attaccante nell'episodio seguente.

Il punto di vista di ***Elliot***

Data/Ora: 3:26 di un martedì mattina del febbraio 1998.
Luogo: stabilimento della Marchand Microsystems, Nashua, New Hampshire.

Elliot Staley sapeva di non dover mai lasciare la sua postazione quando non era in giro di ispezione, però era notte fonda, e non aveva visto una sola persona da quando era montato di servizio. E comunque era quasi l'ora del giro. Il poveretto al telefono sembrava avere **davvero** bisogno di una mano. E uno è sempre contento quando può fare del bene.

La versione di ***Bill***

Bill Goodrock aveva una sola meta nella vita, cui si atteneva adamantino, uno scopo immutato da quando aveva dodici anni: andare "in pensione" a ventiquattro anni senza nemmeno toccare un centesimo del suo fondo fiduciario. Tanto per dimostrare al padre, l'onnipotente e spietato banchiere, che poteva farcela da solo.

Mancavano solo due anni e ormai era perfettamente chiaro che non sarebbe riuscito a fare fortuna nei successivi ventiquattro mesi solo continuando a fare l'affarista rampante, e nemmeno con qualche investimento oculato. Una volta si chiese persino se fosse il caso di mettersi a rapinare le banche a mano armata, ma erano solo favole, il rapporto rischi-benefici era osceno. Invece, sognava a occhi aperti di compiere una rapina elettronica.

L'ultima volta che era andato in Europa con i familiari aveva aperto un conto corrente a Montecarlo con cento franchi, e ancora conteneva solo quei cento miseri franchi, però aveva un progettino per farlo scattare a sei zeri entro breve. E **casomai** anche a sette.

La sua fidanzata Annemarie lavorava per una grande banca di Boston. Un giorno, mentre lui aspettava nell'ufficio di lei in attesa che finisse una riunione, aveva ceduto alla curiosità e aveva attaccato il portatile a una porta Ethernet. Sì! Era entrato nella loro rete interna, nella rete della banca... Oltre il firewall **aziendale.** Gli venne in mente un'idea.

Unì il suo talento a quello di un compagno che conosceva una certa Julia, una brillante dottoranda in informatica che stava facendo uno stage presso la Marchand Microsystems. Sembrava un'ottima fonte per ottenere informazioni cruciali dall'interno. Quando le raccontarono che stavano scrivendo la sceneggiatura di un film, lei abboccò come un pesce. Trovava divertentissimo

creare una storia con loro e fornire tutti i particolari su come portare al successo una mossa come quella che le avevano descritto. La riteneva un'idea brillante, anzi, non la smetteva più di tempestarli di richieste sul suo nome che doveva comparire nel tamburino del film. Loro I'awertirono che spesso le idee per un film vengono rubate, facendole giurare che non l'avrebbe mai detto a nessuno.

Erudito a dovere da Julia, **Bill** si assunse la parte rischiosa senza mai dubitare un istante di potercela fare.

Quando chiamai nel pomeriggio riuscii a scoprire che il responsabile della sorveglianza notturna si chiamava Isaiah Adams. Alle nove e mezza di quella stessa sera chiamai la sede per parlare con la guardia al banco dell'atrio cercando di sembrare in preda al panico e con i minuti contati. "Ho un guasto alla macchina e non posso venire lì, però avrei un'emergenza e ho dawero un gran bisogno che qualcuno mi dia una mano. Ho cercato di chiamare Isaiah, il responsabile, ma non è in casa. Può farmi solo questo unico favore? Le sarei **davvero** grato," dissi.

Tutte le stanze di quella grande struttura avevano un codice, così gli diedi quello del laboratorio informatico e chiesi se sapeva dove si trovava. La guardia rispose di sì e accettò di andarci, dicendo che ci avrebbe messo qualche minuto. Gli spiegai che l'avrei chiamato nel laboratorio adducendo la scusa che stavo usando l'unica linea che avevo a disposizione e mi serviva per cercare di entrare in rete per tentare di risolvere il problema.

Quando chiamai, lui era già **là** che aspettava. Gli dissi dov'era la console che mi interessava e che doveva cercare un foglio con SU scritto "elmer", l'host che secondo Julia usavano lì dentro per preparare le versioni finali del sistema operativo. Appena mi disse che l'aveva trovato ebbi la conferma che Julia ci aveva dato informazioni credibili, e il mio cuore accelerb il battito. Quando gli feci premere Invio un paio di volte lui mi disse che dava il segno #, il che mi confermò che il computer era loggato come root, l'account di superutente con tutti i privilegi di sistema. Il brav'uomo non era molto abile con i tasti ed era tutto preoccupato quando cercai di convincerlo a battere il mio prossimo comando:

```
echo 'fix:x:0:0::/:/bin/sh' >> /etc/passwd
```

Alla fine ci riuscì e così adesso avevamo un account con un "name fix", una correzione di nome. Poi gli feci battere

```
echo 'fix::10300:0:0' >> /etc/shadow
```

Questo stabiliva la password cifrata, quella tra il doppio due punti. Se non ci metti niente in mezzo significa che l'account ha una password nulla. In questo modo erano bastati due comandi per aggiungere la correzione dell'account al file delle password, con una password nulla. Soprattutto, l'account avrebbe avuto i medesimi privilegi come superutente.

Il passo successivo che gli feci compiere fu eseguire un "comando directory ricorsivo" che stampò un lungo elenco di nomi di file, poi gli dissi di portarsi il foglio al banco perché "forse avrò bisogno che me ne legga dei pezzi tra poco".

La bellezza di questa mossa era che l'amico non sapeva di avere creato un nuovo account e io gli avevo anche fatto stampare l'elenco directory dei nomi dei file per essere sicuro che i comandi che aveva dato prima lasciassero la stanza con lui. In quel modo il mattino seguente l'amministratore di sistema o l'operatore non si sarebbero accorti di nulla che potesse far loro subdorare una falla nella sicurezza.

Adesso avevo un account, una password e i privilegi illimitati. Un po' prima di mezzanotte mi collegai e seguii le istruzioni battute coscienziosamenteda Julia "per la sceneggiatura". In un lampo ebbi accesso a uno dei sistemi di sviluppo contenenti la copia master del codice sorgente della nuova versione del sistema operativo lì prodotto.

Caricai un patch scritto da Julia, che secondo lei modificava una routine in una delle librerie del sistema operativo e avrebbe creato una ***backdoor*** segreta per l'accesso remoto al sistema con una password nota solo al sottoscritto.

Seguii attentamente le istruzioni di Julia, prima installando il patch poi rimuovendo il cambiamento di account e cancellando tutti gli audit logs in modo da non lasciare traccia delle mie malefatte, in pratica cancellai le impronte.

In breve tempo, l'azienda avrebbe cominciato a distribuire gli upgrade del nuovo sistema operativo ai suoi clienti, istituti bancari sparsi in tutto il mondo. E ogni copia inviata avrebbe contenuto la backdoor che avevo inserito nel master prima, permettendomi così l'accesso a qualunque sistema informatico di banca o broker che avesse installato l'upgrade.

Ovviamente non avevo ancora finito, restava un po' di lavoro da fare. Dovevo accedere alla rete interna di ogni istituto finanziario che volevo "visitare", poi scoprire quale loro computer veniva usato per i trasferimenti monetari e installare un programma di sorveglianza per imparare i particolari delle loro operazioni e come trasferire fondi con esattezza.

Tutto questo potevo farlo da lontano. Da un computer qualsiasi. Diciamo su una spiaggia. Tahiti, arrivo.

Richiamai il guardiano, lo ringraziai per l'aiuto e gli dissi che poteva buttare la stampata.

Analizziamo l'attacco

La guardia aveva istruzioni sui suoi doveri, ma persino le istruzioni più pignole e meditate non possono prevedere tutte le alternative possibili. Nessuno gli aveva parlato del danno che può essere provocato battendo pochi tasti su un computer per conto di una persona da lui creduta dipendente dell'azienda.

Con la collaborazione della guardia è stato relativamente facile accedere a un sistema cruciale che conteneva il master pronto per la distribuzione, nonostante si trovasse dietro le porte sbarrate di un laboratorio sicuro. Naturalmente la guardia aveva le chiavi di tutte le porte sbarrate.

Persino un impiegato onesto (o in questo caso una dottoranda che faceva uno stage presso l'azienda, Julia) può essere corrotto o ingannato in modo da rivelare informazioni di importanza vitale per un attacco, come per esempio dove si trova il computer bersaglio e (la chiave per il successo di questo tentativo) quando avrebbero completato la nuova versione del programma prima della distribuzione. È importante visto che un cambiamento del genere fatto troppo presto ha maggiori possibilità di essere individuato o annullato se il sistema operativo viene reimpiantato da una fonte pulita.

Avete apprezzato il dettaglio della guardia che prima ha portato la stampata al banco nell'atrio e in seguito l'ha distrutta? È stata una mossa importante. L'attaccante non voleva che gli operatori dei computer scoprissero la prova scottante sul terminale delle stampate o che si accorgessero del contenuto di un cestino una volta arrivati in ufficio il mattino dopo. Fornendo alla guardia una scusa plausibile per portarsela dietro ha evitato questo rischio.

> Quando l'intruso informatico non riesce ad accedere fisicamente a un sistema o a una rete, tenta di convincere un'altra persona a farlo per lui. Nei casi in cui per il suo piano è necessaria la presenza fisica, usare la vittima come intermediario è ancor più soddisfacente che farlo di persona perché per l'attaccante ci sono meno rischi di essere beccato.

IL PATCH DI EMERGENZA

Uno penserebbe che il responsabile dell'assistenza tecnica conosca per filo e per segno i pericoli insiti nel dare accesso alla rete informatica a un esterno. Ma quando l'esterno è un furbo

ingegnere sociale capace di spacciarsi per un premuroso fornitore di programmi, i risultati possono essere diversi da quanto vi aspettate.

Una chiamata di soccorso

Quello all'altro capo del filo voleva sapere chi era il responsabile dei computer del posto, perciò il centralinista lo mise in contatto con uno dell'assistenza tecnica, Paul Ahearn.

L'altro si identificò come: "Edward della SeerWare, il fornitore del database. Sembra che parecchi clienti non abbiano ricevuto le e-mail con il nostro aggiornamento d'emergenza, perciò stiamo chiamando per controllare se c'è stato qualche problema a installare il patch. Avete già installato l'aggiornamento?".

Paul rispose che era abbastanza sicuro di non aver visto nulla del genere.

Allora Edward: "Be', potrebbe causare a intermittenza perdite catastrofiche di dati, perciò raccomandiamo di installarlo appena possibile". Sì, disse Paul, l'avrebbe fatto di sicuro. "Bene, possiamo mandarvi un CD con il patch, ma voglio ricordarle che è **davvero** vitale, due aziende hanno già perso parecchi giorni di dati. Perciò installatelo sul ***serio*** appena arriva, prima che succeda anche a voi," ricordò il sedicente Edward.

"Non posso scaricarlo dal vostro sito **web?**" volle sapere Paul.

"Dovrebbe essere disponibile tra poco, la squadra tecnica ha dovuto risolvere tante beghe. Se vuole possiamo farglielo installare in remoto dal nostro centro assistenza clienti. Possiamo fare in modem o usare Telnet per connetterci al sistema, se lo supportate."

"Non accettiamo Telnet, soprattutto da Internet. Non è sicuro. Se potete usare SSH sarebbe perfetto," disse Paul citando un prodotto che permette il trasferimento sicuro dei file.

"Certo che l'abbiamo. Indirizzo IP?"

Paul glielo diede, e quando Andrew chiese quali username e password poteva utilizzare Paul gli comunicò anche quelli.

Analizziamo l'attacco

Naturalmente la telefonata poteva provenire benissimo dal produttore del database, ma allora questa vicenda non figurerebbe nel presente libro.

In questo caso l'ingegnere sociale ha influenzato la vittima instillando il terrore della perdita di dati vitali e offrendo la soluzione immediata che avrebbe risolto il problema.

Quando un ingegnere sociale prende di mira qualcuno che conosce il valore dell'informazione, deve trovare argomenti molto solidi e persuasivi per ottenere l'accesso remoto. Certe volte deve aggiungere l'elemento dell'urgenza in modo che la vittima sia distratta dalla fretta e ceda prima di avere potuto ponderare la richiesta.

LA NUOVA RAGAZZA

Quale genere di informazioni contenute nei file della vostra azienda potrebbero interessare a un attaccante a tal punto da fare di tutto per accedervi? Certe volte può essere materiale che non pensate di aver bisogno di proteggere.

La telefonata a Sarah

"Risorse umane, sono Sarah."

"Ciao, Sarah, sono George del garage sotterraneo. Hai presente la card che usiamo per entrare nel parcheggio e negli ascensori? Be', abbiamo avuto un problema e dobbiamo riprogrammarle per tutti i nuovi assunti degli ultimi quindici giorni."

"Ti servono i loro nomi?"

"E numeri di telefono."

"Posso controllare l'elenco dei nuovi assunti e richiamarti più tardi. Che numero hai?"

"Sono al 73... Uh, è vero, sto andando in pausa. Che ne dici se ti richiamo tra mezz'ora?"

"Va bene."

Quando lui richiama, Sarah dice: "Ah, sì. Be', sono solo due. Anna Myrtle, alle finanze, segretaria. E il nuovo vicepresidente, il signor Undenvood.

"E i numeri di telefono?"

"Certo... Allora, il signor Undenvood è al 6973. Anna Myrtle ha il **2127.**"

"Mi sei stata di grandissimo aiuto. Grazie."

La telefonata ad Anna

"Finanze, sono Anna."

"Sono felice di avere trovato qualcuno che si trattiene dopo l'orario. Senti, sono Ron Vittaro, servizi editoriali della divisione economia. Non credo ci abbiano ancora presentato. Benvenuta in azienda."

"Oh, grazie."

"Anna, sono a Los Angeles e avrei un'emergenza. Mi servono dieci minuti del tuo tempo."

"Certo. Di cosa ha bisogno?"

"Devi andare nel mio ufficio. Sai dove si trova?"

"No."

"Bene, è quello d'angolo al 15° piano, stanza 1502. Ti chiamo lì tra pochi minuti. Quando arrivi devi premere il pulsante perché la chiamata non passi direttamente in casella vocale."

"Certo, parto subito."

Dieci minuti dopo Anna è nell'ufficio di Vittaro, ha tolto il trasferimento di chiamata e sta aspettando quando squilla il telefono. Lui le dice di sedersi al suo computer e lanciare Internet Explorer, poi di scrivere un indirizzo: **www.geocities.com/ron_insen/manuscript.doc.exe.**

Compare una finestra di dialogo che lui le dice di aprire. Sembra che il computer inizi a scaricare il manoscritto, poi lo schermo si spegne. Quando Anna gli segnala che c'è qualcosa che non va, lui risponde: ***"No,*** di nuovo. Ho problemi ogni tanto a scaricare da quel sito web, però credevo che fosse stato sistemato. Bene, non si preoccupi, recupererò dopo quel file". Poi le chiede di riavviare il computer per essere sicuro che non ci siano malfunzionamenti dopo il problema occorso e le spiega come fare.

Quando il computer funziona di nuovo a puntino la ringrazia calorosamente e appende, così Anna torna nell'ufficio finanze per finire ciò che stava facendo.

La versione di Kurt Dillon

La Millard-Fenton Publishers era entusiasta del nuovo autore che stavano per mettere sotto contratto, l'amministratore delegato di una grandissima azienda appena andato in pensione con una storia affascinante da raccontare. Qualcuno gli aveva consigliato di rivolgersi a un agente per gestire le trattative, ma costui non voleva confessare di non sapere un'acca di contratti editoriali, perciò assunse un vecchio amico perché gli desse una mano a capire che cosa doveva chiedere. Purtroppo il vecchio amico fu una scelta arrischiata. Kurt Dillon usava per le sue ricerche metodi che potremmo definire non ortodossi, non proprio etici.

Per cominciare si abbonnò a un sito gratis su Geocities sotto il nome di Ron Vittaro e vi caricò un programma *spyware*, cambiandone il nome in **manuscript.doc.exe** di modo che sembrasse un documento Word e non destasse sospetti. In realtà funzionò anche meglio del previsto visto che il vero Vittaro non aveva mai

cambiato un'impostazione default nel suo Windows chiamata "Nascondi estensioni per tipi conosciuti di file". A causa di quell'impostazione il file compariva sul serio con il nome manuscript.doc.

Poi Kurt convinse un'amica a chiamare la segretaria di Vittaro, seguendo le sue istruzioni. "Sono l'assistente esecutiva di Paul Spadone, presidente della Ultimate Bookstores di Toronto. Tempo fa il signor Vittaro ha conosciuto il mio principale a una fiera del libro e gli ha chiesto se poteva chiamarlo per discutere un progetto comune. Il signor Spadone è spesso in viaggio, così mi ha chiesto se riuscivo a sapere quando può trovare il signor Vittaro."

Finito di confrontare i programmi, l'amica di Kurt aveva abbastanza informazioni da fornire all'attaccante una lista di date in cui Vittaro sarebbe stato in ufficio. Il che significava che adesso lui sapeva anche quando *non* ci sarebbe stato. Non c'era voluto molto di più per scoprire che la segretaria di Vittaro approfittava di queste assenze per andare a sciare. Per un tot entrambi non sarebbero stati in sede. Perfetto.

Il primo giorno della loro assenza Dillon fece una finta chiamata urgente per verificare, e si senti dire dal centralinista che: "Il signor Vittaro non è in ufficio e nemmeno la sua segretaria. Non li aspettiamo in giornata né domani né dopodomani".

Il suo primo tentativo per convincere una dipendente di basso livello a partecipare al suo piano andò a segno, e la donna non parve battere ciglio quando le spiegò che doveva aiutarlo a scaricare un "manoscritto", che in realtà era un popolare programma spyware disponibile in commercio che l'attaccante aveva modificato per una *installazione silenziosa*. Con questo metodo l'installazione non sarebbe stata rilevata da un antivirus. Per qualche strano motivo i produttori di antivirus non vendono prodotti che rilevano gli spyware in commercio.

Appena la giovane ebbe caricato il programma nel computer di Vittaro, Kurt tornò su Geocities per sostituire il file doc.exe con un manoscritto qualsiasi trovato in Internet. Nel caso qualcuno avesse scoperto l'inghippo e fosse tornato nel sito per indagare cos'era successo, avrebbe trovato solo un innocuo manoscritto amatoriale, impubblicabile.

Una volta installato il programma e riavviato il computer, lo spyware era immediatamente attivo. Ron Vittaro sarebbe tornato dopo qualche giorno, avrebbe iniziato a lavorare e lo spyware avrebbe iniziato a instradare ogni battuta sul computer, comprese tutte le e-mail in uscita e le schermate. Sarebbe stato tutto spedito a intervalli regolari a un provider con servizio gratuito di posta elettronica in Ucraina.

Nel giro di pochi giorni dopo il ritorno di Vittaro, Kurt stava

> Chiedere a un collega o subordinato di farci un favore è pratica comune. Gli ingegneri sociali sanno come sfruttare il desiderio atavico di aiutare e far parte di una squadra, e approfittano di questa tendenza positiva per convincere i dipendenti ignari a compiere azioni che li condurranno più vicini alla meta. È importante comprendere questo semplice concetto per avere maggiori probabilità di rendersi conto quando qualcun altro ci sta manipolando.

sguazzando nei log che si ammassavano nella sua casella postale ucraina e in breve individuò le e-mail riservate che indicavano fino a che punto la Millard-Fenton era disposta ad arrivare nel contratto con l'autore. Con questa notizia in saccoccia, l'agente dell'autore ebbe buon gioco a negoziare termini molto migliori di quanto offerto in origine senza mai correre il rischio di far saltare la trattativa. E questo ovviamente significava una commissione molto più alta per l'agente.

Analizziamo l'attacco

In questo caso l'attaccante ha aumentato le possibilità di successo scegliendo una nuova impiegata che agisse da intermediario, presumendo che sarebbe stata più disposta a collaborare e meno informata della struttura, dei suoi componenti e delle buone pratiche di sicurezza che avrebbero sventato il tentativo.

Visto che Kurt si è fatto passare da vicepresidente nella sua conversazione con Anna, una nuova impiegata, sapeva che era alquanto improbabile che lei mettesse in discussione la sua autorità. Al contrario, poteva pensare che aiutandolo sarebbe stata notata da un boss.

E la procedura attraverso la quale ha guidato Anna ha fatto sì che l'installazione di uno spyware apparisse innocua. Anna non immaginava che delle azioni apparentemente innocenti avrebbero regalato a un attaccante informazioni preziose da usare contro gli interessi dell'azienda.

E perché Kurt ha scelto di inviare i messaggi del vicepresidente a un account di posta elettronica in Ucraina? Una destinazione remota rende per tanti motivi meno probabile rintracciare o fare qualcosa contro un attaccante. Questo genere di reati solitamente viene considerato di bassa priorità in paesi come l'Ucraina, dove la polizia ritiene infrazione poco degna di nota un crimine commesso in Internet. Perciò una casella postale in paesi che difficilmente collaborano con le forze dell'ordine statunitensi è una strategia intelligente.

Un ingegnere sociale preferirà sempre prendere di mira un dipendente che difficilmente intuisce che c'è qualcosa di sospetto nelle sue richieste. Non solo gli rende più facile il lavoro, ma anche meno rischioso, come illustrano gli esempi in questo capitolo.

Ingannare l'ignaro

Ho già sottolineato la necessità di addestrare i dipendenti in modo che non possano essere indotti a seguire le istruzioni di un estraneo. E tutti devono anche capire i pericoli creati da una richiesta di intervento sul computer altrui. La politica aziendale dovrebbe proibirlo tranne quando specificamente approvato da un dirigente. Le situazioni accettabili sono:

- Quando la richiesta è fatta da una persona ben conosciuta, con una domanda a quattr'occhi o per telefono se la voce è riconoscibile senza equivoci.
- Quando si verifica l'identità del richiedente tramite procedure comprovate.
- Quando l'azione è autorizzata da un supervisore o da altra persona provvista di autorità che conosce personalmente il richiedente.

I dipendenti devono essere istruiti a non dare aiuto a persone che non conoscono direttamente, anche se sostengono di essere dirigenti. Una volta approntate le politiche di verifica, la direzione deve aiutare il personale a osservarle, persino se dovesse significare che un dipendente non obbedirà a un dirigente che gli chiede di infrangere una regola.

Ogni azienda deve avere anche alcune procedure che istruiscano il personale su come rispondere alle richieste di intervento su computer o macchine correlate. Nell'episodio della casa editrice l'ingegnere sociale ha preso di mira una nuova assunta che non era stata messa al corrente delle procedure sulla sicurezza delle informazioni. Per prevenire questo genere di attacchi ogni dipendente nuovo o vecchio deve seguire una regola semplice: non usare mai un computer in caso di richiesta da parte di estranei. Punto.

Ricordate che ogni lavoratore con accesso fisico o elettronico a un computer o a uno strumento correlato è passibile di manipolazioni.

Il personale, soprattutto del settore IT, deve capire che per-

mettere l'accesso alle reti informatiche è come dare il numero della propria carta di credito a uno che fa televendite. Il personale deve stare molto attento alle richieste che possono portare allo scoperto informazioni delicate o compromettere il sistema informatico aziendale.

Gli impiegati della IT devono anche stare in guardia contro gli interlocutori sconosciuti che si spacciano come forniton. In genere, un'azienda deve pensare se sia il caso di indicare persone specifiche come contatti per ogni fornitore di tecnologia, imponendo agli altri dipendenti di non rispondere alle richieste dei fornitori di informazioni o cambiamenti sui macchinari telefonici o informatici. In questo modo le persone designate conoscono il fornitore che telefona e viene in visita, ed è meno probabile che si facciano ingannare da un impostore. E se un fornitore chiama anche quando l'azienda non ha un contratto di assistenza, questo atteggiamento deve sollevare automaticamente sospetti.

Tutti i componenti della struttura devono conoscere le minacce alla sicurezza dell'informazione e i punti deboli. Ricordatevi che i custodi e simili devono essere addestrati non solo nella sorveglianza generica ma anche in quella specifica dell'*informazione.* Visto che le guardie hanno spesso libero accesso fisico all'intera struttura, devono saper riconoscere i vari tipi di attacco che possono essere portati contro di loro.

Attenti allo spyware

Una volta lo spyware commerciale era usato soprattutto dai genitori per controllare che cosa facesero i figli in Internet, e dai datori di lavoro, in teoria per vedere che cosa combinavano gli impiegati mentre navigavano in Internet. Un uso un po' più serio era il rilevamento dei potenziali furti di informazioni o lo spionaggio industriale. I progettisti commercializzavano il loro spyware offrendolo come strumento per proteggere i bambini, quando in realtà il vero mercato era rappresentato da persone che desideravano spiare qualcuno. Oggi la vendita di spyware è sostenuta in grandissima parte dal desiderio di sapere se il consorte o amato ti stia tradendo.

Poco prima di iniziare a scrivere la storiella dello spyware in queste pagine, la persona che riceve le e-mai1 per conto mio (visto che non posso usare Internet) ha trovato un messaggio spam che pubblicizzava una serie di prodotti spyware. Un software offerto era descritto come segue:

Eccezionale! Da non perdere: questo potente programma di monitoraggio e spionaggio cattura in segreto ogni digitazione e

il tempo e l'intestazione di tutte le finestre attive di un file di testo, il tutto restando nascosto in sottofondo. I log possono essere cifrati e inviati automaticamente a uno specifico indirizzo di posta elettronica oppure registrati su disco fisso. L'accesso al programma è protetto da password e può essere nascosto dal menu CTRL+ALT+DEL.

Usatelo per monitorare URL, sedute chat, e-mail o tante altre cose (persino password;-)).

Installatelo senza essere scoperti su QUALSIASI PC e mandatevi in posta elettronica i log!!!!!!!

Breccia negli antivirus?

Un antivirus non scopre lo spyware commerciale, perciò lo vede come innocuo anche se serve a spiare. In questo modo, l'equivalente informatico del telefono sotto controllo passa inosservato, creando il rischio di essere tutti quanti sottoposti a sorveglianza illegale in qualsiasi momento. Owiamente, i produttori di antivirus possono ribattere che lo spyware può essere usato per scopi legittimi, e quindi non dovrebbe essere trattato come illegale. Però gli sviluppatori di certi strumenti un tempo utilizzati dagli hacker, e ora liberamente distribuiti o venduti come software di sicurezza, sono ugualmente trattati alla stregua di codici illegali. È una politica del doppio binario, e mi domando perché.

Un altro strumento offerto nella medesima e-mail prometteva di riuscire a catturare le schermate dell'utente, come se ci fosse una telecamera alle sue spalle. Alcuni di questi programmi non richiedono nemmeno l'accesso fisico al computer, basta installare e configurare in remoto l'applicazione e avrete all'istante un computer sotto controllo! L'FBI deve amare la tecnologia.

Essendo così facile procurarsi lo spyware, la vostra azienda deve prevedere due livelli di protezione. Dovete installare un programma di rilevamento spyware come SpyCop (disponibile da www.spycop.com) su tutte le postazioni di lavoro, e dovete richiedere che il personale faccia scansioni periodiche. Inoltre, dovete informare i dipendenti del pericolo di essere convinti a scaricare un programma o di aprire un allegato che potrebbe installare un programma pericoloso.

Oltre a impedire che lo spyware sia installato mentre un impiegato è lontano dalla scrivania per una pausa caffè, a pranzo o in riunione, una politica che imponga a tutti di bloccare il computer con una password salvaschermo o metodi simili abbasserà notevolmente il rischio che persone non autorizzate acce-

dano ai computer. Anche se uno è riuscito a infiltrarsi in un ufficio o cubicolo non potrà accedere ai file, leggere la posta o installare spyware o altri programmi aggressivi. Le risorse necessarie per mettere in funzione una password salvaschermo sono pari a zero, e i vantaggi nella protezione delle postazioni di lavoro sono notevoli. Il rapporto costi-benefici in questo caso è lapalissiano.

13.
Attacchi più elaborati

Ormai avrete capito che quando un estraneo telefona con una richiesta di informazioni scottanti o di qualcosa che potrebbe riuscirgli prezioso, la persona che riceve la chiamata dev'essere preparata a farsi dare il suo numero di telefono e a richiamare per verificare che costui sia **davvero** chi afferma di essere, un dipendente dell'azienda o di una consociata oppure dell'assistenza tecnica di un fornitore, per esempio.

Persino quando una ditta applica una procedura che il personale segue attentamente per verificare chi chiama, gli attaccanti abbastanza sofisticati sono ancora capaci di usare tanti trucchi con cui far credere alla vittima che sono effettivamente chi affermano di essere. Persino i dipendenti **più** attenti alla sicurezza possono essere turlupinati da metodi come questo.

LA FUORVIANTE IDENTIFICAZIONE DI CHIAMATA

Chiunque abbia mai ricevuto una chiamata su un cellulare conosce l'optional dell'identificazione di chiamata, la schermata che mostra il numero di chi vi telefona. In ambito commerciale offre il vantaggio di far capire subito al dipendente se la chiamata viene da un collega o da fuori.

Tanti anni fa alcuni phreaker ambiziosi si sono permessi il lusso dell'identificazione di chiamata ancora prima che il servizio fosse disponibile al pubblico e se la spassarono facendo scherzi alla gente tipo rispondere e salutare l'altro per nome anche prima che dicesse una parola.

Proprio quando pensate di essere al sicuro grazie alla verifica dell'identità fidandovi di quel che vedete, cioè di quanto appare sul display, l'attaccante colpisce.

La telefonata a Linda

Giorno/Ora: martedì 23 luglio, ore 15:12
Luogo: uffici del settore finanze, Starbeat Aviation.

Il telefono di Linda Hill squillò proprio mentre stava scrivendo un appunto per il capo. Controllò la chiamata, che veniva dall'ufficio di New York, anche se era da parte di un certo Victor Martin, un nome sconosciuto.

Pensò di lasciarla alla segreteria per non essere costretta a interrompere, però a un certo punto vinse la curiosità, e così sollevò la cornetta. L'altro si presentò dicendo che era delle pubbliche relazioni e stava preparando del materiale per il presidente. "Sta andando a Boston per colloqui con le banche e ha bisogno del bilancio di questo trimestre. Ah, un'altra cosa. Vuole anche le proiezioni finanziarie sul progetto Apache," aggiunse Victor, usando il nome in codice di un prodotto che sarebbe stato una delle proposte fondamentali della compagnia per la primavera.

Quando lei gli chiese l'indirizzo di e-mail, il sedicente Victor rispose di avere un problema a riceverle pèrché c'erano i tecnici al lavoro. Poteva faxargliele? Appena Linda acconsentì le diede l'interno corrispondente al suo fax.

Lei lo spedì pochi minuti dopo.

Peccato che Victor non lavorasse per le pubbliche relazioni. Anzi, non lavorava nemmeno per quell'azienda.

La versione di Jack

Jack Dawkins aveva iniziato sin da ragazzino come borseggiatore allo Yankee Stadium, sulle affollate piattaforme della metropolitana e fra i turisti serali in Times Square. S'era dimostrato così lesto di mano e pieno di risorse da poter sfilare l'orologio dal polso della vittima senza che questa nemmeno se ne accorgesse. Purtroppo nel corso della sua impacciata adolescenza aveva perso la mano leggera e s'era fatto beccare. Nel carcere minorile aveva imparato un nuovo mestiere con minori rischi di essere preso.

Il suo incarico attuale consisteva nell'ottenere il più recente bilancio di un'azienda, più le informazioni sui ricavi, prima che i dati fossero inviati alla commissione di Borsa diventando di pubblico dominio. Il suo cliente era un dentista che non voleva spiegare come mai gli servivano quelle informazioni. Secondo Jack era una prudenza risibile. Ne aveva viste tante, forse quello aveva problemi al tavolo da gioco oppure un'amichetta costosa di cui la moglie non sapeva nulla. O forse si era appena vantato

con la consorte di quanto era bravo a giocare in Borsa, e adesso aveva perso una cifra e voleva piazzare un grosso investimento su un'azienda sicura sapendo in anticipo se le azioni sarebbero salite una volta presentati i risultati trimestrali.

La gente normale ci rimane quando scopre quanto poco tempo serve a un ingegnere sociale intraprendente per risolvere una situazione inaspettata. Quando Jack tornò dal suo appuntamento con il dentista aveva già un piano. Il suo amico Charles Bates lavorava per la Panda Importing, una ditta provvista di un centralino privato o PBX.

Secondo una terminologia familiare a chi ne sa qualcosa di sistemi telefonici, il PBX era collegato a un servizio di telefonia digitale noto come T1, configurato come Primary Rate Interface ISDN (Integrated Services Digital Network) o PRI ISDN. In parole povere, ogni volta che telefonavano dalla Panda, le informazioni per l'elaborazione della chiamata uscivano lungo un canale che andava fino alla centralina dell'azienda telefonica, e comprendevano il numero del chiamante inviato (a meno di non essere bloccato) al meccanismo di identificazione della chiamata del ricevente.

L'amico di Jack sapeva come programmare il centralino in modo che la persona ricevente vedesse non il vero numero di telefono alla Panda ma qualsiasi altro numero inserito, un trucco che funziona sempre perché le compagnie telefoniche locali non si curano di confrontare il numero di chiamata ricevuto dal cliente con i veri numeri per cui l'abbonato paga le bollette.

A Jack Dawkins bastava accedere a un servizio telefonico del genere. Per fortuna il suo amico e talvolta socio Charles Bates era sempre felice di dargli una mano per un compenso nominale. In questo caso riprogrammarono in via transitoria il centralino dell'azienda in modo che le chiamate da una data linea nella sede della Panda simulassero l'interno di Victor Martin e una telefonata dalla Starbeat Aviation.

L'idea che l'identificazione di chiamata possa mostrare il numero che ti pare è tanto poco risaputa che di rado questo servizio viene messo in dubbio. In questo caso Linda fu felice di faxare l'informazione richiesta al tizio che credeva appartenesse alle pubbliche relazioni.

Quando Jack appese, Charles riprogrammò il centralino della Panda per ripristinare l'originale impostazione del numero.

Analizziamo l'attacco

Alcune aziende non vogliono che i clienti o i fornitori sappiano i numeri di telefono dei dipendenti. Per esempio, la Ford può decidere che le chiamate dal loro centro assistenza clienti deb-

bano mostrare il prefisso del numero verde e una dizione tipo "Assistenza Ford invece del vero numero diretto del responsabile che fa la telefonata. La Microsoft potrebbe permettere ai dipendenti di dare il proprio numero invece di lasciare che tutti i riceventi vedano l'identificazione di chiamata. In questo modo l'azienda può mantenere la riservatezza degli interni.

Però questa possibilità di riprogrammare regala una scappatoia pratica per lo scherzomane, per il recupero crediti, per quello delle televendite e ovviamente per l'ingegnere sociale.

VARIAZIONE SUL TEMA: C'È AL TELEFONO IL PRESIDENTE DEGLI STATI UNITI

Come co-conduttore di una trasmissione radiofonica, *Il* lato *oscuro* di Zntemet, su KFI Talk Radio di Los Angeles, ho lavorato sotto l'egida del direttore della programmazione dell'emittente, David, uno dei più grandi lavoratori che abbia mai conosciuto, difficilissimo da raggiungere per telefono essendo sempre molto occupato. È uno di quelli che rispondono solo se leggono sull'identificazione di chiamata che è una persona con cui devono parlare per forza.

Quando lo chiamavo, avendo il blocco sul mio cellulare, lui non sapeva mai chi stava telefonando e quindi non rispondeva, perciò venivo dirottato sulla segreteria, cosa molto frustrante.

Ne parlai con un vecchio amico cofondatore di un'immobiliare che scova uffici per le ditte di hi-tech, e assieme escogitammo un piano. Lui aveva accesso al centralino della sua azienda, un Meridian che consente di programmare il numero, come descritto nel caso precedente. Ogni volta che dovevo raggiungere il direttore della programmazione e non ci riuscivo, chiedevo al mio amico di programmare il numero di mia scelta che doveva comparire nell'identificatore. Certe volte la facevo sembrare come se venisse dal suo assistente, altre dalla holding proprietaria dell'emittente.

La mia preferita era la chiamata che sembrava provenire dal suo numero di casa, a cui lui rispondeva sempre. Però devo ammetterlo, era sempre gentile quando rispondeva e scopriva che l'avevo fregato un'altra volta. La parte migliore era che poi restava in linea abbastanza da sentire che cosa desideravo.

Quando ho spiegato questo trucchetto all'Art Bell Show ho fatto in modo che l'identificatore mostrasse nome e numero della sede di Los Angeles dell'FBI. Art è rimasto scosso dalla trovata, e mi ha tirato le orecchie perché stavo facendo una cosa illegale, ma io gli ho ricordato che è perfettamente legale fino a quando non commetti una frode. Dopo il programma ho ricevuto parec-

chie centinaia di e-mail che mi chiedevano di spiegare come si faceva. Adesso lo sapete.

È lo strumento ideale per regalare credibilità all'ingegnere sociale. Se per esempio durante la fase di ricerca dell'attacco scopre che il bersaglio ha l'identificatore, può falsificare il numero in modo che sembri provenire da una ditta o dipendente fidato. Un esattore può far apparire che la chiamata arrivi dall'ufficio della vittima.

> La prossima volta che vi telefonano e l'identificatore di chiamata vi mostra che viene dall'adorata mamma... be', potrebbe essere un adorato ingegnere sociale.

Però fermatevi un attimo a riflettere sulle implicazioni. Un intruso informatico può chiamarvi a casa sostenendo di essere del settore IT della vostra impresa, e di avere un bisogno urgente della password per ripristinare i vostri file dopo un crash di server. Oppure l'identificatore mostra nome e numero della vostra banca o broker di Borsa, e quella ragazza dalla voce suadente ha solo bisogno di verificare i numeri di conto e il cognome da ragazza della mamma. Per buona misura vorrebbe verificare il PIN del Bancomat a causa di problemi al sistema. Un team di operazione d'attacco in Borsa può far in modo di figurare come se chiamasse dalla Merrill Lynch o dalla Citibank. Potrebbe chiamare qualcuno che vuole rubarvi l'identità, in apparenza telefonando dalla Visa e convincendovi a dargli il numero di carta di credito. Un tipo rancoroso potrebbe sostenere di essere un federale o del fisco.

Se avete accesso a un sistema telefonico collegato a un PRI più quel pizzico di competenza di programmazione che potete acquisire dal sito web del fornitore del sistema, potete usare questa tattica per fare divertenti scherzi agli amici. Conoscete qualcuno con esagerate ambizioni politiche? Potete programmare il numero di riferimento 202 456-1414, e l'identificatore indicherà "Casa Bianca".

Sarà convinto che lo stia chiamando il presidente!

La morale della storia è semplice: non fidarsi mai dell'identificazione di chiamata, se non quando la si usa per le chiamate interne. Sia a casa sia in ufficio tutti devono essere al corrente di questo trucco e sapere che nome e numero che compaiono sul display non devono essere dati per scontati quando si tratta di verificare l'identità.

LA DIPENDENTE INVISIBILE

Shirley Cutlass ha trovato una nuova maniera divertente per fare soldi in fretta. Basta con le interminabili ore alla catena. Si è unita alle centinaia di artisti della truffa coinvolti nel crimine del decennio. Adesso è una ladra di identità.

Oggi ha preso di mira le informazioni confidenziali del settore servizi per la clientela di una compagnia di carte di credito. Dopo i soliti compiti a casa, chiama la compagnia vittima e chiede al centralinista che risponde di essere messa in contatto con le telecomunicazioni, dove domanda del responsabile delle caselle vocali.

Usando le informazioni raccolte durante le ricerche sostiene di chiamarsi Norma Todd della sede di Cleveland. Poi utilizzando un trucco che ormai dovrebbe esservi familiare, afferma che tra una settimana arriverà alla sede centrale e avrà bisogno di una mailbox vocale per non essere costretta a fare lunghe interurbane per controllare i messaggi registrati nella sua. Non c'è bisogno di una connessione telefonica fisica, basta solo una casella vocale. L'uomo risponde che ci penserà lui e che la richiamerà quando sarà tutto sistemato per darle gli estremi.

Lei ribatte con voce seducente: "Sto andando in riunione, posso richiamarla tra un'ora?".

Quando lei richiama, l'amministratore dice che è tutto a posto e le dà le informazioni, l'interno e la password temporanea, e le chiede se sa come cambiare la password della segreteria, così Shirley l'ascolta compita mentre l'amministratore spiega la procedura, anche se la conosce bene quanto lui.

"A proposito, dall'albergo quale numero devo chiamare per controllare i messaggi?" chiede Shirley. L'altro le dà il numero.

Lei telefona, cambia la password e registra il suo nuovo saluto in uscita.

Shirley *attacca*

Finora è stato facile. Adesso è pronta a usare l'arte dell'inganno.

Chiama il settore servizi alla clientela dell'azienda. "Sono delle riscossioni della sede di Cleveland," dice, poi lancia una variante della scusa ormai familiare. "L'assistenza mi sta sistemando il computer e ho bisogno del vostro aiuto per avere un'informazione." Poi fornisce nome e data di nascita della persona di cui sta rubando l'identità elencando le informazioni che vuole: indirizzo, cognome da ragazza della madre, numero di carta di credito e scadenza, credito disponibile e movimenti. "Mi richiami a questo numero, e se non ci sono lasci pure detto in segreteria," conclude, dando l'interno preparato per lei dall'amministratore delle caselle vocali.

Ha da fare per il resto della mattinata, perciò controlla la segreteria solo nel pomeriggio. C'è tutto quello che ha chiesto. Prima di appendere, Shirley cancella il messaggio in uscita. Sarebbe un errore lasciarsi alle spalle la registrazione della sua voce.

E il furto di identità, il reato a maggior tasso di crescita in America, il crimine "in" del nuovo secolo, sta per fare un'altra vittima. Shirley usa le informazioni sulla persona e sulla carta di credito appena ottenute per iniziare ad addebitare alla vittima.

Analizziamo l'attacco

In questa truffa l'attaccante ha prima ingannato il responsabile delle caselle vocali dell'azienda facendogli credere di essere una dipendente per cui allestire una voice mailbox transitoria. Se si fosse premurato di controllare, l'uomo avrebbe scoperto che il nome e il numero di telefono forniti corrispondevano a quelli nel database aziendale.

Il resto è stato solo questione di dare una scusa ragionevole su un problema informatico, chiedere le informazioni desiderate e pregare che la risposta fosse lasciata in segreteria. Perché mai un impiegato dovrebbe essere riluttante a condividere informazioni con una collega? Dato che il numero di telefono fornito da Shirley era chiaramente un interno, non c'era motivo di sospettare.

> Provate a chiamare la vostra casella vocale ogni tanto. Se sentite un messaggio in uscita diverso dal vostro, forse avete appena incontrato il vostro primo ingegnere sociale.

LA COLLABORAZIONE DELLA SEGRETARIA

Il cracker Robert Jorday entrava di continuo nelle reti informatiche di una multinazionale, la Rudolfo Shipping Inc. Alla fine l'azienda si accorse che qualcuno violava il loro terminal server e che attraverso quello poteva collegarsi con qualsiasi sistema interno. Per salvaguardare la rete, la Rudolfo decise di richiedere una "modem password su ogni terminal server.

Robert chiamò il centro operazioni rete [Noc–Network Operations Center] spacciandosi per un avvocato del settore legale e accampando problemi di connessione. L'amministratore di rete che raggiunse gli spiegò che c'erano stati problemi di sicurezza, quindi adesso tutti gli utenti da modem dovevano ottenere la password mensile dal loro direttore. Robert si domandò allora quale metodo usavano per comunicare la password mensile ai direttori e come ottenerla. Scopri allora che la password del mese successivo sarebbe stata spedita per posta interna.

Questo semplificava le cose. Robert fece qualche ricerca, quindi chiamò l'azienda subito dopo il primo del mese raggiun-

L'ingegnere sociale dotato è molto bravo a **influenzare** la gente affinché gli faccia un favore. Ricevere un **fax** e inoltrarlo altrove sembra una cosa tanto innocua che è elementare convincere una persona al banco d'accoglienza a farlo per noi. Quando qualcuno chiede un favore che **riguarda** le informazioni, se non lo conoscete né potete accertare la sua identità, ditegli di no.

gendo la segretaria di un **capoufficio,** Janet. "Ciao, Janet, sono Randy Goldstein della ricerca e sviluppo. So che devo aver ricevuto la nota con la password mensile per collegarsi al server da fuori, però non la trovo da nessuna parte. Tu l'hai ricevuta?"

Janet confermò.

Quando Robert le chiese se poteva gentilmente mandargliela per **fax,** lei disse di sì. Perciò le diede il numero di fax del banco d'accoglienza in un diverso edificio della sede centrale, dove s'era già messo d'accordo che gli tenessero i facsimili e **glieli** rimandassero. Però stavolta usò un nuovo metodo per farsi rimbalzare il fax, dando alla ricezionista un numero che andava su un servizio **fax online,** che in automatico riceve un **facsimile** e lo invia **all'indirizzo** di e-mail dell'abbonato.

La nuova password arrivò nella casella di posta elettronica che Robert aveva aperto presso un servizio gratuito in Cina. Era sicuro che anche se avessero rintracciato il fax, l'investigatore avrebbe avuto gravi problemi a ottenere la collaborazione dei funzionari cinesi che secondo lui erano più riluttanti che amichevoli in materie del genere. E soprattutto non era costretto ad apparire fisicamente sul punto d'arrivo del fax.

IL TRIBUNALE DEL TRAFFICO

Penso che chiunque sia stato multato per eccesso di velocità abbia sognato a occhi aperti la maniera di scamparla. Non certo prendendo altre lezioni di scuola guida o banalmente pagando la multa oppure cercando di convincere il giudice con qualche cavillo tecnico tipo quand'è stata l'ultima volta che hanno controllato l'autovelox o il tachimetro della volante. No, l'ipotesi **più** affascinante è quella di fregare il sistema.

La truffa

Anche se non raccomanderei a nessuno di provare questo metodo per non pagare una multa (come si dice sempre, non provatelo a casa), è però un ottimo esempio di come l'arte **dell'inganno** può aiutare l'ingegnere sociale.

Il nostro violatore del codice stradale lo chiameremo Paul Durea.

Primi passi

"Polizia di Los Angeles, distretto Hollenbeck."
"Salve, vorrei parlare con chi controlla i mandati di comparizione."
"Sono io."
"Perfetto. Sono l'awocato John Leland, dello studio Meecham, Meecham e Talbot e dovrei chiedere la comparizione di un agente in una causa."
"Va bene. Quale agente?"
"C'è un Kendall nella vostra stazione?"
"Numero di matricola?"
"21349."
"Sì. Per quando le serve?"
"Il mese prossimo, però dovrei far comparire parecchi altri testimoni e poi dire al giudice i giorni buoni. Ci sono giorni il prossimo mese in cui l'agente Kendall è impegnato?"
"Vediamo... È in ferie dal 20 al 23, e ha l'addestramento l'8 e il 9."
"Grazie. Per ora mi basta. La richiamo quando hanno fissato il giorno in aula."

Tribunale cittadino, segreteria

Paul: "Vorrei programmare la comparizione in aula per una multa".
Impiegato: "Va bene, posso assegnarle il 26 del mese prossimo".
"Bene. Vorrei presentare una contestazione."
"Una contestazione della multa?"
"Sì."
"D'accordo. Possiamo fissarla per domani mattina o pomeriggio. Cosa preferisce?"
"Pomeriggio."
"Contestazione domani all'una e mezza aula 6."
"Grazie, ci sarò."

Tribunale cittadino, aula 6

Data: giovedì, 13:45.
Segretario: "Signor Durea, prego, si avvicini al banco".

Giudice: "Signor Durea, ha capito i diritti che le sono stati spiegati oggi pomeriggio?".

Paul: "**Sì,** Vostro onore".

"Preferisce le lezioni di guida? La denuncia sarà ritirata dopo il completamento effettivo di otto ore di corso. Ho controllato la sua fedina penale e attualmente risulta idoneo."

"No, Vostro onore. Con rispetto chiedo il processo. Un'altra cosa, Vostro onore. Sarò in viaggio, ma dovrei essere libero l'8 o il 9. Sarebbe possibile fissare il processo uno di questi due giorni? Domani parto per lavoro per l'Europa e torno tra quattro settimane."

"Benissimo. Processo fissato l'8 giugno, ore otto e trenta, aula 4."

"Grazie, Vostro onore."

Tribunale cittadino, aula 4

L' 8 Paul arrivò presto in tribunale. Quando entrò il giudice il segretario gli consegnò la lista dei casi in cui gli agenti non si erano presentati. Il giudice chiamò gli imputati e li informò che il caso era chiuso.

Analizziamo l'attacco

Un agente rilascia una multa la firma con il nome e numero di matricola (o come si chiama il numero personale nella sua struttura). Trovare a quale stazione appartiene è una passeggiata, basta una telefonata alle informazioni abbonati citando la struttura di tutela dell'ordine che compare nella citazione (stradale, ufficio dello sceriffo o altre) per avere già un piede infilato nella porta. Contattata questa agenzia, potete ottenere l'esatto numero di telefono della segreteria mandati dell'area in cui è stata elevata la multa.

I tutori dell'ordine devono comparire in aula con regolarità, fa parte del loro lavoro. Quando un procuratore distrettuale o un difensore ha bisogno della loro deposizione, se sa come funziona il sistema, controlla per prima cosa i giorni in cui l'agente è libero. E facile, basta chiamare l'impiegato dei mandati di comparizione della sua stazione o distretto.

Di solito durante queste conversazioni l'avvocato chiede se l'agente sarà libero nella tal data. Invece per questo giochetto Paul ha avuto bisogno di un minimo di tatto, doveva trovare una ragione plausibile perché l'impiegato gli spiegasse in quali date l'agente non era disponibile.

Quando andò per la prima volta in tribunale perché non disse

semplicemente al segretario quale data voleva? Facile: da quel che mi risulta, di solito i segretari di tribunale non permettono al pubblico di scegliere la data. Se quella suggerita dal segretario non va bene, allora sarà offerta qualche alternativa, ma è il massimo che possono fare. D'altro canto, uno che è disposto a sprecare tempo a farsi vivo per una contestazione è possibile sia più fortunato.

Paul sapeva di avere diritto a una contestazione. E sapeva che i giudici sono spesso disposti **a** cedere in caso di richiesta di una data specifica. Chiese con scrupolo le date coincidenti con i giorni in cui l'agente era impegnato nell'addestramento sapendo che nel suo stato questi giorni avevano la precedenza sulle comparizioni in aula.

> La mente umana è un'invenzione meravigliosa. È interessante notare quanto riesca a essere creativa la gente quando si tratta di inventare modi subdoli per ottenere quanto le pare o per togliersi da una situazione spinosa. Dovete usare la medesima creatività e immaginazione per proteggere i sistemi informatici e di informazione nei settori pubblici e privati. Perciò, gente, quando pensate alle politiche di sicurezza delle vostre aziende... siate creativi e pensate fuori dal sentiero tracciato.

E nelle cause per infrazioni al traffico quando l'agente non si presenta... la causa è chiusa. Nessuna multa. Niente lezioni di guida. Nessun punto negativo sulla patente. E soprattutto nessuna registrazione di infrazioni!

Secondo me alcuni poliziotti, commessi di tribunale, procuratori distrettuali e simili che leggono queste pagine scuoteranno tristemente il capo perché sanno perfettamente che questo trucchetto funziona. Però scuotere la testa è il massimo che possono fare. Non cambierà nulla. Ci scommetterei. Come dice Cosmo nel film del 1992 ***I signori*** *della truffa:* "È solo questione di uno e zero," per far capire che alla fine tutto si riduce all'informazione.

Fino a quando le varie polizie sono disposte a dare informazioni sugli impegni degli agenti praticamente a tutti coloro che chiamano, sarà sempre possibile non pagare le multe. Avete brecce simili nelle procedure della vostra azienda, varchi che un astuto ingegnere sociale può sfruttare per avere informazioni che preferireste non arrivassero nelle sue mani?

LA VENDETTA DI SAMANTHA

Samantha Gregson era arrabbiata.

Aveva lavorato duro per la laurea, accumulando molti debiti con il mutuo studenti. Le avevano sempre detto che il pezzo di

carta ti regalava una professione al posto di un lavoro, i soldi veri. E invece laureatasi in amministrazione non aveva trovato un impiego decente.

Perlomeno era abbastanza contenta di aver ricevuto quell'offerta della Lambeck Manufacturing. Certo, era umiliante accettare il posto di segretaria, ma il signor Cartright le aveva spiegato che erano molto soddisfatti di averla con loro, e che quel posto da segretaria l'avrebbe messa sulla rampa di lancio non appena liberatosi un posto in amministrazione.

Due mesi dopo aveva saputo che uno dei vicedirettori di Cartright se ne andava. Quella notte non aveva quasi chiuso occhio immaginandosi già al quinto piano, in un ufficio con una porta, a partecipare a riunioni e prendere decisioni.

Il mattino dopo si recò subito dal signor Cartright, il quale le disse che secondo loro Samantha doveva imparare altre cose sul settore prima di essere adatta per una posizione dirigenziale. Infine, assunsero un dilettante esterno che ne sapeva meno di lei.

Fu allora che cominciò a capire: l'azienda era imbottita di donne ma erano quasi tutte segretarie. Non le avrebbero mai dato un incarico dirigenziale. Mai.

Ritorsione

Ci mise quasi una settimana per pensare come fargliela pagare. Circa un mese prima, un tale di una rivista specializzata l'aveva raggirata quando era passato da loro per il lancio di un nuovo prodotto. Qualche settimana dopo l'aveva chiamata in ufficio dicendo che se gli avesse mandato informazioni sul nuovo Cobra 273 le avrebbe spedito un mazzo di fiori e se poi erano notizie scottanti valide per un articolo sarebbe venuto apposta da Chicago per portarla fuori a cena.

Pochi giorni dopo Samantha era nell'ufficio del giovane Johansson quando questi si collegò con la rete aziendale. Senza nemmeno stare a pensarci, gli guardò le dita (il cosiddetto "shoulder surfing", spiare una persona che digita per rubarle la password o altre informazioni). Johansson aveva battuto "marty63" come password.

Il piano stava cominciando a prendere forma. Ricordava ancora di aver battuto un comunicato poco dopo il suo anivo in azienda. Ne trovò una copia nello schedario e ne batté una nuova versione imitando il linguaggio del primo. Diceva:

A: C. Pelton, uff. IT
DA: L. Cartright, Sviluppo

> Martin Johansson lavorerà con un gruppo progetti speciali del mio dipartimento.
> Quindi l'autorizzo ail'accesso ai server usati dal gruppo progettazione. Il profilo di sicurezza del signor Johansson dev'essere aggiornato per garantirgli i medesimi diritti ail'accesso in quanto sviluppatore del prodotto.
>
> Louis Cartright

Quando erano quasi tutti a pranzo Samantha tagliò la firma del signor Cartright dal comunicato originale, l'incollò sulla nuova versione e sbianchettò i bordi, poi fece una fotocopia e una copia della copia. Adesso non si notavano più le ombre attorno alla firma.

Poi mandò il **fax** dalla macchina accanto all'ufficio del signor Cartright.

Tre giorni dopo si trattenne fino a tardi aspettando che uscissero tutti, quindi entrò **nell'ufficio** di Johansson cercando di entrare in rete con i suoi **username** e password, **marty63**. Funzionò.

Dopo pochi minuti aveva localizzato i file con le specifiche del prodotto Cobra **273,** scaricandoli su uno Zip.

Il dischetto era al sicuro nella sua borsetta quando uscì al fresco vento della sera in pieno parcheggio. In serata sarebbe partita per andare a trovare quel giornalista.

Analizziamo l'attacco

Un dipendente insoddisfatto, una ricerca nei file, una veloce operazione di taglia e incolla e sbianchetta, un po' di copiaggio creativo e un **fax.** Voilà! Aveva sotto gli occhi le segretissime notizie sul prodotto e sul marketing.

Pochi giorni dopo un giornalista di una rivista del settore aveva il suo scoop con le specifiche e i piani di marketing di un nuovo articolo innovativo, dettagli che sarebbero finiti nelle mani degli abbonati con mesi di anticipo rispetto all'uscita del prodotto. Le aziende concorrenti avrebbero avuto parecchie settimane di vantaggio per sviluppare prodotti equivalenti e preparare una campagna di stampa per controbattere Cobra **273.**

Naturalmente la rivista non rivelerà mai la fonte del proprio scoop.

PREVENIAMO GLI ATTACCHI

I dipendenti devono sapere che, quando si chiede loro un'informazione preziosa, delicata o vitale che potrebbe **avvan-**

taggiare un concorrente o altri, l'identificazione di chiamata come metodo per verificare l'identità di chi telefona da fuori non è sufficiente. Devono usare metodi diversi di verifica, come per esempio controllare presso il superiore di costui che sia una richiesta corretta e che l'utente sia autorizzato a ricevere quell'informazione.

La procedura di verifica esige un equilibrio che ogni azienda deve trovare da sola: sicurezza a scapito della produttività. Quale priorità assegnare all'applicazione delle misure di sicurezza? I membri del personale saranno restii contro le procedure di sicurezza o addirittura le aggireranno pur di svolgere il loro lavoro? Capiscono perché la sicurezza è importante per l'azienda e per loro? Occorre rispondere a queste domande se si vuole approntare una politica della sicurezza basata sulla cultura aziendale e sulle necessità commerciali.

Tanta gente vede come una seccatura tutto ciò che interferisce con l'esecuzione del proprio lavoro e aggira le misure di sicurezza che le sembrano uno spreco di tempo. La chiave giusta è motivare il personale tramite educazione e informazione affinché la sicurezza diventi parte integrante delle mansioni quotidiane.

Anche se il servizio di identificazione della chiamata non dovrebbe mai essere usato come metodo di conferma delle telefonate a voce da fuori, un altro metodo denominato identificazione automatica del numero (ANI) invece può. È un servizio fornito quando un'azienda si abbona per utenze tipo numero verde in cui è lei a pagare le telefonate in arrivo, ed è affidabile. A differenza dell'identificazione di chiamata, il centralino della compagnia dei telefoni non usa le informazioni inviate dal cliente quando fornisce il numero. Quello indicato dall'ANI è il vero numero assegnato all'utente.

Ricordate inoltre che parecchi produttori di modem hanno aggiunto nelle loro macchine un'opzione identificazione che protegge la rete aziendale permettendo le chiamate in accesso remoto solo da un elenco di numeri autorizzati. I modem con identificazione di chiamata sono un mezzo accettabile di autentica in un ambiente a bassa sicurezza ma, come avrete ormai capito, manipolarli è relativamente facile, quindi non ci si dovrebbe affidare a essi per verificare un'identità o una localizzazione negli ambienti a massima sicurezza.

Per risolvere il problema del furto d'identità, come nella storia in cui hanno convinto un responsabile di servizio a creare una mailbox vocale sul sistema telefonico aziendale, prevedete che tutti i servizi telefonici, tutte le caselle vocali e tutti gli accessi all'elenco aziendale, su carta o in rete, debbano essere richiesti per iscritto su un modulo apposito. La domanda dev'es-

sere firmata dal capoufficio del richiedente, e l'amministratore delle segreterie vocali dovrà verificare la firma.

La politica di sicurezza aziendale deve prevedere che i nuovi account o l'allargamento dei diritti di accesso siano concessi solo dopo verifica positiva della persona richiedente, come una telefonata al direttore o amministratore di sistema o suo delegato al numero specificato sull'elenco aziendale stampato o online. Se l'impresa usa le e-mail sicure in cui i dipendenti possono firmare digitalmente i messaggi, anche questa verifica alternativa può essere accettata.

Ricordate sempre che qualsiasi dipendente, che abbia accesso o no ai sistemi informatici aziendali, può essere ingannato da un ingegnere sociale. Tutti devono passare dal training specifico per la sicurezza. Segretari, addetti al ricevimento, centralinisti e guardie devono diventare esperti delle forme più probabili di attacco, per essere meglio preparati a difendersi.

14.
Spionaggio industriale

La pericolosità degli attacchi alle informazioni di enti statali, grandi imprese e università è ben nota. Quasi ogni giorno i giornali ci raccontano di un nuovo virus, blocchi del servizio o furti dei dati sulle carte di credito da un sito di e-commerce.

Sappiamo di casi di spionaggio industriale come quando la Borland ha accusato la Symantec di rubare segreti commerciali, o la Cadence Design Systems ha denunciato il furto del codice sorgente da parte di un concorrente. Tanti uomini d'affari leggono questi articoli credendo che alla loro azienda non potrebbe mai accadere.

Invece succede ogni giorno.

VARIAZIONE SUL TEMA

Il raggiro descritto nel racconto seguente dev'essere stato tentato parecchie volte, anche se sembra tolto di peso da un film hollywoodiano come Insider o dalle pagine di un romanzo di John Grisham.

Causa collettiva

Immaginate un'enorme causa collettiva contro una grande azienda farmaceutica, la Pharmomedic. Secondo la denuncia, l'azienda era al corrente del fatto che uno dei suoi farmaci più venduti aveva effetti collaterali devastanti, ma che uscivano allo scoperto solo quando il paziente assumeva il farmaco da anni, e la Pharmomedic aveva i risultati di numerosi studi che eviden-

ziavano questo rischio ma li aveva tenuti nascosti senza mai passarli come d'obbligo alla FDA.

William "Billy" Chaney, awocato eponimo dello studio legale di New York che patrocina la causa collettiva. ha le testimonianze di due medici della Pharmomedic che confermano la denuncia. Perb sono tutti e due in pensione e non hanno uno straccio di documentazione e quindi non sarebbero testimoni forti, convincenti. Billy sa di non avere granché in mano. A meno di non riuscire a entrare in possesso di una di quelle relazioni o di una comunicazione tra due dirigenti, perderà la causa.

Perciò assolda una ditta già utilizzata in passato: Andreeson e Figli, investigatori privati. Non sa come facciano Pete e collaboratori a ottenere la loro roba, né vuole saperlo. Sa solo che Pete Andreeson è un eccellente detective.

Per Andreeson un incarico del genere è quel che lui chiama un lavoro in nero. La sua prima regola è che gli studi legali e le aziende che lo assoldano non devono sapere come fa a ottenere informazioni, in modo da non essere assolutamente imputabili. Se c'è qualcuno che vedrà i sorci verdi sarà Pete, il quale ritiene che valga la candela con quel che guadagna con incarichi del genere. Tra l'altro, lui ricava una soddisfazione personale quando può fregare i furbacchioni.

Se i documenti che Chaney desidera esistono realmente e non sono stati distrutti, saranno negli archivi della Pharmomedic. Perb trovarli negli enormi schedari di una grande multinazionale è un compito immane. D'altro canto è possibile che abbiano dato delle copie ai propri legali, lo studio Jenkins e Petry. Se gli avvocati della difesa sanno che questi documenti esistono e non li consegnano durante le indagini preliminari, allora violano il codice professionale e anche la legge. Secondo Pete, un comportamento del genere rende giusto qualsiasi attacco.

*L'attacco di **Pete***

Pete incarica un paio di ragazzi di fare alcune ricerche, e così nel giro di pochi giorni scopre a quale ditta si rifanno Jenkins e Petry per stoccare i materiali d'archivio, e sa che questa struttura conserva una lista dei nomi che lo studio legale autorizza al prelievo dei nastri. Sa anche che ciascuna di queste persone ha una sua password. Manda così un paio di ragazzi per un lavoretto in nero.

I due scassinano la serratura con una macchinetta comprata in rete su www.southord.com. Nel giro di pochi minuti, diciamo verso le tre di notte, entrano negli uffici della ditta di deposito materiali e accendono un personal. Viene loro da sorridere ve-

dendo il logo di Windows 98 perché ciò significa che sarà un gioco da ragazzi. Windows 98 non richiede alcuna forma di autentica. Dopo un po' di ricerche trovano un database Microsoft Access con i nomi delle persone autorizzate dai clienti al prelievo dei nastri, e aggiungono un nome falso alla lista di Jenkins e Petry, corrispondente a quello che figura sulla patente falsa procurata da uno dei due. Potevano invece entrare di scasso nel deposito e cercare di localizzare i nastri in questione? Certo, ma a quel punto tutti i clienti, compreso lo studio legale, si sarebbero accorti dello scasso. E gli attaccanti avrebbero perso un vantaggio. Ai professionisti piace sempre lasciare una porta aperta per un ingresso futuro, casomai si rivelasse necessario.

Fedeli a una regola classica dello spionaggio industriale di tenere qualcosa in serbo per utilizzi futuri, fanno anche una copia su dischetto del file contenente l'elenco delle persone autorizzate. Non sanno se servirà mai, ma è uno di quei tipici "giacché siamo qui, facciamolo" che ogni tanto torna comodo.

Il giorno dopo uno dei due chiama la ditta di deposito usando il nome aggiunto all'elenco e la password corrispondente, chiedendo tutti i nastri Jenkins e Petry dell'ultimo mese e annunciando che sarebbe passato un fattorino a prenderli. A metà pomeriggio Andreeson ha i nastri in mano. I suoi collaboratori scaricano i dati nel loro sistema informatico, pronti a cercare con comodo. Andreeson è molto contento che lo studio legale, come quasi tutti, non si sia scomodato a cifrare i dati di back-up.

I nastri vengono restituiti al magazzino il giorno dopo e nessuno saprà mai niente.

> Le informazioni di valore devono essere protette in qualsiasi forma o luogo. Un elenco clienti ha lo stesso valore che sia su carta o in forma di file, in ufficio o in archivio. Gli ingegneri sociali preferiscono sempre il punto di attacco più facile da penetrare, il meno difeso. Una struttura esterna di archivio è considerata un luogo dove è più difficile essere visti o scoperti. Ogni organizzazione che deposita dati di valore, delicati o critici presso terzi dovrebbe cifrarli per proteggerne la riservatezza.

Analizziamo l'attacco

Per colpa delle falle nella sicurezza fisica, i "cattivi" non hanno avuto alcun problema a entrare con lo scasso nel deposito, arrivare al computer e modificare il database con l'elenco delle persone autorizzate ad accedere all'unità di stoccaggio. L'aggiunta di un nome all'elenco ha permesso agli impostori di ottenere i nastri di back-up che cercavano, senza nemmeno dover commettere un furto ai danni del deposito. Dato che

molte imprese non cifrano i dati di back-up, le informazioni erano alla loro mercé.

Questo caso è un altro esempio di un fornitore che non mette in atto delle ragionevoli precauzioni, permettendo così all'attaccante di compromettere le informazioni del cliente.

IL NUOVO PARTNER COMMERCIALE

Gli ingegneri sociali hanno un grande vantaggio sui truffatori, la distanza. Un dritto può fregarvi solo se è a quattr'occhi, *e* in quel modo dopo potete dare i suoi connotati oppure addirittura far intervenire la polizia se subodorate in tempo la truffa in corso.

Gli ingegneri sociali evitano come la peste questo rischio. Però certe volte è un rischio necessario, giustificato dalla potenziale ricompensa.

La versione di Jessica

Jessica Andover era contentissima del suo lavoro presso una rampante azienda impegnata nella robotica. Certo, era solo una start-up e pagava pochino, però era piccola, i colleghi simpatici e c'era il piacere aggiuntivo di sapere che le sue stock option potevano renderla ricca. Vabbè, forse non milionaria quanto i fondatori, ma comunque abbastanza agiata.

Quel martedì mattina d'agosto Rick Daggot entrò nell'atrio con un sorriso che andava da un orecchio all'altro. Con quel completo costoso (Armani) e il pesante orologio d'oro massiccio (Rolex President) più un taglio di capelli impeccabile, aveva quell'aria mascolina e sicura di sé che faceva impazzire le liceali.

"Buongiorno, sono Rick Daggot e devo vedere Larry," disse.

Il sorriso di Jessica si spense immediatamente. "Larry? Larry è in vacanza, questa settimana."

"Ho un appuntamento con lui all'una. Sono appena arrivato in volo da Louisville proprio per incontrarlo," insistette Rick, estraendo il Palm e mostrandoglielo.

Jessica controllò scuotendo il capo. "Il 20 è la settimana ***prossima***."

Allora il sedicente Rick riprese il palmare e lo guardò meglio. "Oh no, che fesseria ho commesso."

"Posso prenotarle almeno il volo di ritorno?" chiese Jessica, dispiaciuta.

Mentre lei telefonava, Rick confessò di essere in trattative con

Larry per un'alleanza strategica di marketing. L'azienda di Rick produceva materiali per le linee di montaggio, che si ingranavano alla perfezione con il nuovo prodotto di Larry, il C2Alpha. Messi insieme, i prodotti di Rick e il C2Alpha avrebbero formato un binomio imbattibile che avrebbe aperto importanti mercati industriali per entrambe le imprese.

Quando Jessica ebbe prenotato un posto su un volo del tardo pomeriggio, Rick disse: "Be', almeno potrei parlare con Steve se c'è". Purtroppo il vicepresidente e cofondatore dell'azienda non era in ufficio.

Rick, flirtando un tantino con Jessica, suggerì allora che, essendo ormai lì e avendo un volo solo nel tardo pomeriggio, non gli sarebbe dispiaciuto invitare a pranzo qualche responsabile del progetto. E aggiunse: "E naturalmente anche te. C'è qualcuno che può sostituirti all'ora di pranzo?".

Arrossendo compiaciuta per l'invito, Jessica gli chiese chi desiderava nello specifico. Lui premette ancora qualche tasto sul palmare, poi fece alcuni nomi, due tecnici della ricerca e sviluppo, il nuovo tipo del settore vendite e marketing e quello del settore finanze distaccato al progetto. Suggerì inoltre che fosse lei a introdurre i rapporti di Rick con l'azienda, ma che poi gli sarebbe piaciuto presentarsi da solo. Dopo aver proposto il migliore ristorante dei paraggi, un posto dove Jessica aveva sempre desiderato andare, disse che avrebbe prenotato per mezzogiorno e mezzo e che avrebbe richiamato in mattinata per verificare che fosse tutto a posto.

Incontratisi al ristorante (gli altri quattro più Jessica), il tavolo non era ancora pronto, perciò si fermarono al bar dove Rick chiarì che erano tutti suoi ospiti. Era una persona di classe, di quelle che ti fanno subito sentire a tuo agio, come se lo conoscessi da anni. Aveva sempre la cosa giusta da dire, la battuta pronta quando la conversazione languiva e ti faceva desiderare la sua attenzione.

Rivelò sufficienti particolari sui suoi prodotti da delineare la soluzione di joint venture che pareva eccitarlo tanto, e citò parecchie grandi aziende cui già vendeva finché tutti i presenti cominciarono a immaginarsi il loro prodotto diventare un successone appena uscito di fabbrica.

Poi Rick si dedicò a Brian, uno dei tecnici. Mentre gli altri discutevano tra loro, ebbe uno scambio di vedute con Brian lasciandolo parlare degli aspetti rimarchevoli del C2Alpha e di quanto lo distingueva dalla concorrenza. Scoprì così un paio di dettagli che l'azienda taceva ma di cui Brian sembrava molto fiero.

Rick proseguì in quel modo con gli altri, mentre sostavano al bar, discutendo simpaticamente con ciascuno. Quello del mar-

keting pareva lieto di avere la possibilità di parlare della data di distribuzione e dei piani commerciali. E il contabile estrasse una busta dalla tasca per mettere nero su bianco i dettagli di costi di produzione, prezzo al pubblico e margini previsti, e delle condizioni contrattabili con ogni venditore, che elencò.

Quando il tavolo fu pronto Rick aveva già discusso con tutti e si era fatto parecchi ammiratori. Alla fine del pasto tutti gli strinsero la mano e lo ringraziarono. Rick scambiò con ciascuno il biglietto da visita e ***en passant*** disse a Brian, il tecnico, che voleva discuterne ancora appena tornava **Larry.**

Il giorno seguente, quando rispose al telefono, Brian si ritrovò Rick, il quale affermava di avere appena avuto uno scambio di opinioni con Larry. "Torno da voi lunedì per decidere qualche specifica con lui, ma intanto vuole che sappia tutto del vostro prodotto e dice che dovresti mandargli per posta elettronica gli ultimi progetti e specifiche. Deciderà lui le parti che devo avere prima di spedirmele."

Quando il tecnico confermò che si poteva fare, Rick rispose: "Ottimo. **Larry** voleva farti sapere che ha un problema con le e-mail. Invece di mandarla sul suo solito account, s'è messo d'accordo con l'albergo che gli ha aperto un account su Yahoo. Dovresti mandare i file a larryrobotics@yahoo.com."

Quando il lunedì mattina Larry arrivò in ufficio abbronzato e sereno, Jessica non vedeva l'ora di parlargli di Rick. "Che tipo eccezionale. Ci ha invitati a pranzo, persino me." Larry pareva perplesso. "Rick? Chi diavolo è Rick?"

"Ma come, il suo nuovo partner."

"Che cosa???!!!"

"E tutti sono rimasti impressionati dalle sue domande."

"**Non** conosco nessun Rick..."

"Ma cosa dice? Se è uno scherzo, Larry, non è divertente."

"Voglio subito la dirigenza in sala riunioni. ***Subito.*** Non **m'interessa** se hanno da fare. E tutti quelli che erano presenti al pranzo. Compresa lei."

Si sedettero rabbuiati al tavolo, pressoché muti. Larry entrò, si sedette e annunciò: "Non conosco nessun Rick. Non ho un nuovo partner che vi sto tenendo nascosto. Pensavo fosse ovvio. Se c'è un burlone tra voi, voglio che parli ***subito".***

Non si sentì volare una mosca. La stanza sembrava diventare più buia ogni secondo che passava.

Alla fine Brian chiese: "Perché non ha detto niente quando le ho mandato la **mail** con le specifiche del prodotto e il codice sorgente?".

"***Quale*** **mail?!**"

Brian si irrigidì. "Oh... cazzo."

Cliff, l'altro tecnico, intervenne dicendo: "Ha dato a tutti il

suo biglietto da visita. Basta chiamarlo per sapere che cosa sta combinando".

Brian aprì il palmare, premette un tasto e lo passò a Larry. Tutti i presenti, ancora speranzosi nonostante l'evidenza, guardarono in trance il capo mentre componeva il numero. Dopo un attimo Larry attivò il viva voce per far sentire a tutti il segnale di occupato. Dopo parecchi tentativi nell'arco di venti minuti, lo scoraggiato Larry domandò alla centralinista di chiedere l'interruzione di chiamata.

Qualche secondo dopo la centralinista gli domandò con aria di sfida come avesse avuto quel numero. Larry le spiegò che era sul biglietto da visita di un tale che doveva sentire con urgenza. Allora lei ribatté: "Mi dispiace, ma è il numero collaudo dell'azienda telefonica. Dà sempre occupato".

Larry iniziò a stilare l'elenco delle informazioni passate a Rick. Non era un quadro allegro.

Poi arrivarono due investigatori della polizia per il primo verbale ma, dopo aver sentito i fatti, precisarono che non erano stati commessi reati di loro competenza e non potevano farci nulla. Consigliarono a Larry di contattare l'**Fbi**, avendo loro la giurisdizione sui crimini riguardanti il commercio interstatale. Quando Rick Daggot aveva chiesto al tecnico di spedire il risultati dei test facendosi passare per un altro forse aveva commesso un reato federale, però Rick doveva verificare con il Bureau.

Tre mesi dopo Larry era in cucina a leggere il giornale a colazione quando il caffè gli andò di traverso. Ciò che temeva, da quando aveva saputo di Rick, s'era verificato. Il suo peggior incubo era lì nero su bianco, sulla prima pagina della sezione economica. Un'azienda sconosciuta stava annunciando l'uscita di un nuovo prodotto che sembrava esattamente il **C2Alpha** che loro stavano sviluppando da due anni.

Quei maledetti li avevano battuti con l'inganno. I suoi sogni erano distrutti. I milioni di dollari investiti nella ricerca e sviluppo persi. E con molta probabilità non aveva la minima prova in mano.

La versione di Sammy Sanford

Abbastanza in gamba da poter aspirare a un ottimo stipendio con un lavoro legale, ma nello stesso tempo abbastanza deviato da preferire sbarcare il lunario con le stangate, Sammy Sanford se la cavava piuttosto bene. Era stato notato da una spia costretta al pensionamento anticipato a causa dei suoi problemi di alcolismo e che, rancorosa e amareggiata, aveva trovato la maniera di vendere i talenti in cui il governo l'aveva reso esperta. Sem-

pre in cerca di persone da sfruttare, lo spione aveva inquadrato Sammy fin dal primo momento in cui l'aveva conosciuto. E Sammy aveva trovato facile, e alquanto fruttuoso, passare dal furto dei soldi della gente al furto dei segreti delle aziende.

Molti non avrebbero fegato a fare quel che faccio io. Se provate a fregare la gente al telefono o in Internet quelli non vedono che faccia avete. Ma ogni bravo dritto, uno della vecchia scuola che lavora a quattr'occhi (e ce ne sono ancora molti in circolazione, più di quel che credete), può guardarti in faccia, spararti una panzana e farti credere quel che gli pare. Conosco alcuni giudici che lo ritengono reato. Io credo sia una dote naturale.

Però non puoi arrivare alla cieca, prima devi prendere le misure. Con una truffa di strada puoi saggiare il polso di un pollo con due chiacchiere tra amici e un paio di suggerimenti ben architettati. Poi arrivano le risposte giuste e... tombola! Hai il pollo nel sacco.

Invece un lavoretto con un'azienda appartiene a ciò che noi definiamo il "giro grosso". Devi programmare, scoprire dov'è la stanza dei bottoni e cosa vogliono. Di cosa hanno bisogno. Pianificare un attacco. Essere paziente, fare ricerche. Capire quale parte reciterai e provare le battute. E non entrare da quella porta finché non sei pronto.

Ho speso più di tre settimane per questo colpo. Il cliente mi ha tenuto due giorni in seduta per spiegare quello che faceva la "mia" azienda e come descrivere i tanti motivi per cui sarebbe stata un'alleanza fruttuosa.

Ed ebbi il colpo di fortuna. Chiamai l'altra ditta dicendo di far parte di una struttura di capitali di rischio, e che eravamo interessati a un incontro e stavo organizzando gli appuntamenti per trovare un giorno nei due mesi successivi in cui tutti i soci erano disponibili, perciò volevo sapere se c'era un periodo da evitare, giorni in cui Larry era via. La donna spiegò che, in effetti, il capo non aveva fatto ferie da due anni, da quando cioè era sorta la struttura, ma adesso sua moglie se lo portava a giocare a golf la prima settimana d'agosto.

Mancavano solo due settimane. Potevo attendere.

Intanto, una rivista specializzata del settore tecnologico mi rivelò il nome della ditta responsabile delle pubbliche relazioni dell'azienda, cui dissi che mi piaceva il risalto che riuscivano a dare al loro cliente specializzato nella robotica, e aggiunsi di voler parlare con il loro uomo per coinvolgerlo anche con la mia azienda. Scoprii che questi era una giovane donna dinamica interessatissima a un nuovo cliente. Durante un pranzo costoso bagnato da un bicchierino di troppo, la signorina cercò di con-

vincermi che loro erano bravissimi a comprendere i problemi di comunicazione del cliente e a scoprire le soluzioni giuste. Ce la misi tutta per convincerla, avevo bisogno di dettagli. Grazie a qualche sollecitazione da parte mia, a fine pasto mi aveva raccontato più cose del nuovo prodotto e dei problemi aziendali di quanto sperassi.

La faccenda procedette sul velluto. L'escamotage di apparire imbarazzato perché avevo sbagliato la settimana *dell'appuntamento* nonché l'idea che già che c'ero potevo incontrare la squadra, fu ingoiato amo e lenza dalla ragazza al banco, che era persino dispiaciuta per me. Il pranzo mi costò centocinquanta verdoni con la mancia. Ma avevo quel che mi serviva. Numeri di telefono, incarichi e un tipo in posizione cruciale che mi pendeva dalle labbra.

Ammetto che Brian è stato un problema. In un primo momento era sembrato il genere di persona che mi avrebbe spedito tutto ciò che volevo, e invece sembrava asserragliarsi appena affrontavo l'argomento. Paga sempre prevedere l'imprevedibile. L'account a nome di Larry lo tenevo di riserva. Quelli della sicurezza Yahoo stanno ancora aspettando che qualcuno lo usi di nuovo per poterlo rintracciare. Aspetteranno a lungo. La musica è finita. Adesso posso passare a un altro progetto.

Analizziamo l'attacco

Chiunque architetti una truffa faccia a faccia deve calzare una maschera che lo renda accettabile al bersaglio. Ne indosserà una quando deve farsi vedere all'ippodromo, un'altra per il baretto frequentato dalla preda, un'altra ancora nel locale raffinato di un albergo elegante.

Con lo spionaggio industriale funziona più o meno allo stesso modo. Un attacco può comportare giacca e cravatta e ventiquattr'ore costosa se per caso la spia recita la parte del dirigente di una grande azienda, del consulente o del responsabile vendite. Se invece deve presentarsi come progettista di software o tecnico o impiegato, i vestiti, l'uniforme, il look saranno diametralmente opposti.

Per infiltrare quell'azienda, il tipo che si faceva chiamare Rick Daggot sapeva di dover emanare un'aura di competenza e fiducia nei propri mezzi, sostenuta dalla perfetta conoscenza dei prodotti e della filosofia aziendale.

Non è stato molto difficile mettere le mani sulle informazioni di cui aveva bisogno per cominciare. Ha escogitato un discreto trucco per scoprire quando il gran capo era via. Più difficile, ma non tanto, è stato scoprire i dettagli sul progetto per sembrare

"addentro". Spesso queste informazioni sono note a molti fornitori e investitori, a quelli dei capitali di rischio contattati per i finanziamenti, alle banche e allo studio legale. Però l'attaccante deve stare attento: trovare qualcuno che può rivelare notizie riservate può essere difficoltoso, ma rivolgersi a due o tre fonti per scoprire chi può essere spremuto come un limone fa correre il rischio che, prima o poi, qualcuno mangi la foglia. È pericoloso. I Rick Daggot di questo mondo devono essere scrupolosi e mai battere due volte la stessa strada.

Anche il pranzo è stato un momento abbastanza delicato. Intanto, c'era il problema di fare in modo di restare a tu per tu per qualche minutò con ciascuno, senza essere sentito dagli altri. A Jessica aveva detto alle dodici e mezza ma in realtà il tavolo era prenotato per l'una in quel ristorante costosissimo del genere conto spese. In quel modo, il falso Rick sperava di avere il tempo di bere qualcosa al bar, come in effetti è successo. L'occasione ideale per passare dall'uno all'altro facendo due chiacchiere.

Però ci sono sempre tante possibilità di commettere un passo falso, di dare una risposta sbagliata, di farsi sfuggire una frase inopportuna che rischia di smascherarlo. Soltanto una spia industriale estremamente sicura di sé e molto scaltra può correre il rischio di esporsi in quel modo. Per sua fortuna, gli anni delle truffe di strada l'avevano affinato, regalandogli una gran faccia tosta e la sicurezza di riuscire a fugare qualunque sospetto anche in caso di errore. È stato il momento più pericoloso dell'intera operazione, e il sollievo quando ha portato a buon fine una stangata come questa gli ha fatto capire come mai non era costretto a guidare auto da corsa o fare paracadutismo o tradire la moglie: si divertiva troppo con il suo lavoro. Quante persone possono dire altrettanto?

Che cosa induce un gruppo di uomini e donne in gamba ad

Anche se la maggior parte degli attacchi è condotta per telefono o posta elettronica, non date per scontato che l'attaccante ardito non si farà mai vivo di persona in azienda. Nella maggior parte dei casi, l'impostore usa qualche trucco tipico dell'ingegneria sociale per entrare in un edificio, dopo avere falsificato il tesserino di riconoscimento con un programma diffusissimo come Photoshop. E i biglietti da visita con le linee collaudo dell'azienda dei telefoni? ***Rockford,*** una serie di telefilm su un detective privato, ha mostrato una tecnica astuta e in un certo senso divertente. Rockford (interpretato da James Garner) ha in auto una macchina portatile che stampa biglietti da visita e che usa per produrre i cartoncini utili per l'occasione. Oggigiorno un ingegnere sociale può farseli stampare in un'ora in qualsiasi copisteria o farseli da solo con la stampante laser.

accettare un impostore? Noi valutiamo una situazione con l'istinto e il ragionamento. Se la storia fila (questa è la parte ragionata) e un truffatore riesce a proiettare un'immagine credibile, di solito finiamo con l'abbassare la guardia. E l'immagine credibile a distinguere il truffatore di successo da quello che viene subito smascherato.

Chiedetevi quanto siete sicuri di non abboccare mai a una storia come quella di Rick. Se siete certi che non succederà, domandatevi allora se qualcuno vi ha ***mai*** fregati. Se la risposta alla seconda domanda è sì, probabilmente è anche la risposta esatta alla prima domanda.

GIOCARE ALLA CAVALLINA

Una sfida: la seguente storiella non parla di spionaggio industriale. Mentre la leggete vedete se riuscite a capire come mai l'ho inserita in questo capitolo!

Harry Tardy era tornato a vivere dai suoi, ed era molto amareggiato. I marine erano sembrati un'ottima carta fino a quando non era stato silurato dal corso. Adesso era tornato nella cittadina che odiava, seguiva un corso di informatica al college locale e cercava una maniera per fare il colpo grosso.

Alla fine gli venne in mente un piano. Mentre beveva qualche birra con un collega di corso, lamentandosi del loro istruttore (un so-tutto-io arrogante), avevano escogitato in combutta un piano intricato per farlo fuori: avrebbero rubato il codice sorgente di un popolare PDA (Persona1 Digital Assistant) per farlo arrivare sul computer del tipo, organizzando la questione in modo da lasciare una pista affinché l'azienda danneggiata pensasse che il ladro fosse lui.

Il suo nuovo amico, Karl Alexander, sosteneva di "conoscere qualche trucchetto", perciò avrebbe spiegato a Harry come riuscirci. Senza rischi.

Compiti a casa

Qualche ricerca preliminare svelò a Harry che il prodotto era stato creato presso il Centro sviluppo nella sede oltreoceano del produttore, però c'era anche una struttura per la ricerca e lo sviluppo negli Stati Uniti. Perfetto, spiegò Karl, perché per il buon funzionamento del colpo doveva esserci una sede statunitense che aveva bisogno di accedere al source code.

A quel punto Harry era pronto a chiamare all'estero, e in que-

sti casi viene buona la carta della pietà "Oddio, sono nei pasticci, ho bisogno di una mano, per favore, per favore, mi aiuti". Naturalmente doveva essere qualcosa leggermente più raffinata. Karl scrisse anche un copione, ma quando Harry lo lesse suonò fasullo. Alla fine, si allenò con l'amico in modo da riuscire a spiegare di che cosa aveva bisogno con una certa disinvoltura.

Arrivato il momento, disse qualcosa del genere con Karl seduto accanto: "Chiamo dalla ricerca e sviluppo di Minneapolis e il nostro server si è beccato un worm che ha infettato l'intero dipartimento. Ci è toccato reinstallare il sistema operativo ma una volta ripristinato dal back-up non è bastato. Indovini chi doveva controllare l'integrità dei back-up? Il sottoscritto. Quindi il capo mi ha mangiato vivo e la direzione è incavolata per la perdita dei dati. Senta, avrei bisogno dell'ultima revisione del codice sorgente appena possibile. Vorrei che *gzippasse* [archiviare più file in uno solo compresso, grazie a una utility Gnu Linux; ***N.d.A.***] il codice sorgente e me lo mandasse".

A quel punto Karl scrisse in fretta una frase, così Harry aggiunse, rivolto al tipo con cui stava parlando, che bastava trasferire il file internamente, alla ricerca e sviluppo di Minneapolis. Era un dettaglio importantissimo: appena l'altro capì che gli chiedevano soltanto di trasferire il file a un altro settore dell'azienda si tranquillizzò. Cosa c'era di male?

Quindi accettò di mandare lo Gzip. Passo dopo passo, con Karl a fianco, Harry accompagnò l'interlocutore lungo la procedura di compressione dell'enorme source code in un unico file compattato e gli diede anche il nome da assegnare al file compresso, "newdata", spiegando che in questo modo avrebbero evitato confusioni con i vecchi dati rovinati.

Karl fu costretto a spiegare il passo successivo due volte prima che Harry lo comprendesse, però era essenziale per questa partita alla cavallina inventata dall'amico. Harry doveva chiamare Minneapolis dicendo di voler inviare un file, mentre loro dovevano mandargli qualcos'altro, ovviamente il tutto accompagnato da scuse per farlo sembrare plausibile. Harry era piuttosto confuso perché doveva dire "io vi sto mandando un file" quando invece non era affatto lui che lo mandava. Doveva far credere al tipo della ricerca e sviluppo che il file arrivava da lui mentre invece là avrebbero ricevuto il source code proprietario dall'Europa. "Perché devo dirgli che arriva da me quando invece viene dall'altra parte dell'Oceano?" domandò al complice.

"Il tipo a Minneapolis è il fulcro della faccenda. Deve credere di fare solo un favore a un collega qui in America, che sta ricevendo un file da te e poi lo rimbalza," spiegò Karl.

Alla fine Harry comprese, così chiamò Minneapolis e domandò alla centralinista di essere messo in collegamento con il

centro informatico, dove chiese di poter parlare con un operatore. Venne al telefono un tale che sembrava un coetaneo. Harry lo salutò, gli spiegò che chiamava dal reparto assemblaggio dell'azienda, a Chicago, e che stava cercando di inviare un file a un partner, sebbene "abbiamo un problema con il router e non riesco ad accedere alla loro rete. Vorrei spedire il file a lei, poi quando l'ha ricevuto le telefono per dirle come inoltrarlo al computer del partner".

Fin qui tutto bene. Quindi Harry chiese al giovanotto se il suo centro informatico aveva un *account anonimo* FTP, un'impostazione che permette di trasferire file da e per una cartella senza bisogno di password. Si, era disponibile, così l'altro diede a Harry l'indirizzo IP interno per raggiungerlo.

Con questa informazione in saccoccia Harry richiamò il centro sviluppo in Europa. A quel punto il file compresso era pronto, così Harry diede le istruzioni per trasferire il file al sito anonimo FTP. In meno di cinque minuti il file compresso del source code arrivò al ragazzo alla ricerca e sviluppo.

Incastrare la vittima

Eravamo a metà strada. Adesso prima di procedere, Harry e Karl dovevano aspettare di essere sicuri che il file fosse arrivato, e nell'attesa andarono alla scrivania dell'esercitatore dall'altra parte della stanza per prowedere agli altri due passaggi necessari. Prima installarono un server anonimo FTP sulla sua macchina, la destinazione finale del file.

La seconda mossa forniva la soluzione a un problema altrimenti complesso. Chiaramente non potevano dire al tipo di Minneapolis di inviare un file a un indirizzo tipo warren@rms.ca.edu. Il suffisso .edu tradisce immediatamente, visto che qualsiasi persona minimamente pratica lo riconoscerebbe come l'indirizzo di un ateneo o simili e l'operazione salterebbe in un batter d'occhio. Per evitarlo, entrarono nel Windows per rintracciare l'indirizzo IP della macchina, che sarebbe diventato quello per ricevere il file.

Intanto era già venuta l'ora di richiamare l'operatore alla ricerca e sviluppo. Quando fu al telefono Harry disse: "Ho appena trasferito il file che dicevo. Può controllare se è arrivato?". Sì, era arrivato. Allora Harry gli chiese di provare a inoltrarlo dandogli l'indirizzo IP, e rimase al telefono finché il giovanotto iniziò a trasmetterlo, poi i due complici guardarono con un sorrisone la luce sul drive del computer dell'istruttore dall'altra parte della stanza lampeggiare e lampeggiare, impegnata a scaricare.

Harry fece ancora due chiacchiere con il tipo su come un giorno computer e periferiche sarebbero diventati più affidabili, poi ringraziò e salutò.

I due copiarono il file dalla macchina del nemico su un paio di Zip, uno a testa, per darci un'occhiata in seguito, come se avessero rubato un quadro dal museo per goderselo ma non osassero farlo vedere agli amici. Solo che in questo caso era più come prendere una copia del dipinto, mentre al museo restava sempre l'originale.

Poi Karl spiegò a Harry come rimuovere il server FTP dalla macchina e cancellare le tracce in modo che non restassero prove del crimine, soltanto il file rubato, lasciato dove poteva essere facilmente reperibile.

Come passo conclusivo, postarono una sezione del codice sorgente su Usenet direttamente dal computer della vittima. Solo una parte, per non recare grave nocumento all'azienda, però lasciando chiare tracce che portavano direttamente alla vittima. Avrebbe avuto i suoi problemi a giustificarsi.

Analizziamo l'attacco

Anche se c'è voluta una combinazione di vari elementi per far funzionare questa bravata, non poteva andare a buon fine senza l'abile ricorso alla carta della simpatia e della pietà: il mio boss mi mangia vivo e la direzione è incavolata ecc. Questo, assieme alla spiegazione lucida di come la persona all'altro capo del filo poteva dargli una mano a risolvere il problema, si è dimostrato un raggiro assolutamente convincente. Ha funzionato in questo caso come tante altre volte.

Il secondo elemento cruciale: l'uomo che conosceva il valore del file si è sentito chiedere di inviarlo a un indirizzo ***interno.***

Terzo tassello: l'operatore vedeva benissimo che il file gli era inviato da dentro. Poteva solo significare, almeno così sembrava, che colui che gliel'aveva inviato l'avrebbe spedito alla destinazione finale soltanto se la sua connessione alla rete esterna fosse stata in funzione. Che cosa c'era di male ad aiutare quella persona spedendolo in sua vece?

E la storia del file compresso con un nome cambiato? Pare un tocco marginale, e invece è importante. L'attaccante non poteva permettersi il rischio del file che arrivava con un nome che l'avrebbe identificato al volo come source code o relativo al prodotto. La richiesta di inviare il file con un nome del genere fuori dalla compagnia avrebbe fatto scattare il campanello d'allarme. Una ridenominazione con un nome innocuo era essenziale. Come previsto dagli attaccanti, il secondo giovanotto non ha avuto

> La regola fondamentale che ogni dipendente deve ficcarsi bene in testa è: non passate mai file a persone che non conoscete direttamente, anche se la destinazione è interna alla rete aziendale, se non su conferma della dirigenza.

remore a inviare il file all'esterno. Un file con un nome come "newdata" che non dava indizi sulla vera natura del contenuto non l'avrebbe insospettito.

Per finire, avete capito che cosa c'entra questo episodio in un capitolo sullo spionaggio industriale? Se la risposta è no eccovi la spiegazione: questi studenti hanno fatto uno scherzo che poteva essere organizzato tranquillamente da una spia industriale professionista, forse pagata da un concorrente o da un governo straniero. Come che sia, il danno poteva essere tremendo per l'azienda, compromettendo gravemente le vendite del nuovo prodotto una volta che quello della concorrenza fosse uscito sul mercato.

Un attacco del genere potrebbe essere portato anche contro la vostra impresa?

PREVENIAMO GLI ATTACCHI

Lo spionaggio industriale, da sempre un pericolo per gli affari, è diventato il pane quotidiano delle spie tradizionali che si sono riciclate nel campo furti a pagamento di segreti aziendali dopo la fine della Guerra fredda. Oggi i governi stranieri e le multinazionali usano spie industriali freelance per rubare informazioni. Anche le aziende interne assoldano dei broker di informazioni che varcano il confine della legalità per ottenere dati cruciali. Sono innumerevoli i casi di ex spie militari riciclate come broker dotati di un'esperienza e una competenza tali che permettono loro di sfruttare facilmente le varie organizzazioni, soprattutto quelle che non sono riuscite a impiantare salvaguardie adatte a proteggere le informazioni e a educare il personale.

Sicurezza fuori sede

Che cosa poteva salvare l'azienda che ha avuto problemi con la struttura esterna di deposito? In questo caso il danno poteva essere evitato se avessero cifrato i dati. Certo, la codifica significa tempo e spese in più, però vale lo sforzo. I file crittati devono essere controllati con regolarità per verificare che la codifica/decodifica proceda a dovere.

C'è sempre il pericolo che le chiavi di crittaggio vadano per-

dute o che l'unica persona che le conosce finisca sotto un tram, però questi inconvenienti possono essere minimizzati. Tutti coloro che conservano informazioni delicate presso un'altra ditta e non usano la codifica sono, scusate la franchezza, degli idioti. È come andare a fare due passi in un quartiere malfamato con delle banconote che spuntano dalla tasca, in pratica è come chiedere di essere rapinati.

Lasciare i supporti del back-up dove chiunque può prenderli è una classica falla della sorveglianza. Parecchi anni fa sono stato dipendente di un'azienda che poteva sforzarsi un po' di più di proteggere le informazioni sui clienti. Il personale lasciava i nastri di back-up fuori dalla stanza computer sbarrata e un fattorino li raccoglieva ogni giorno. Chiunque poteva sottrarre questi nastri che contenevano tutti i documenti in chiaro elaborati al word processor della ditta. Se i dati di back-up sono cifrati, la perdita del materiale è un fastidio, se non lo sono... be', capite meglio di me le conseguenze per la vostra azienda.

È abbastanza assodata la necessità nelle grandi aziende di un affidabile stoccaggio esterno. Però le procedure di sicurezza devono comprendere un'indagine sulla struttura di deposito per analizzare il loro grado di attenzione procedurale. Se non sono attenti quanto la vostra impresa, tutti i vostri sforzi rischiano di essere compromessi.

Le piccole imprese hanno una discreta alternativa al back-up: inviare ogni sera i file nuovi e quelli cambiati a una struttura che offre archivio in rete. Anche qui è essenziale che i dati siano cifrati, altrimenti le informazioni sarebbero a disposizione non solo di un dipendente corrotto della ditta di stoccaggio, ma anche di ogni intruso in grado di infiltrarsi nei sistemi informatici o nella rete di deposito online.

Owiamente se allestite un sistema di codifica per proteggere la sicurezza dei file di riserva, dovete anche pensare a una procedura di massima sicurezza per conservare le chiavi di crittaggio o le passphrase che le sbloccano. Le chiavi segrete usate per cifrare i dati dovrebbero essere conservate in cassaforte o in un caveau. La procedura standard deve prevedere la possibilità che il dipendente gestore di questi dati se ne vada all'improvviso, muoia o passi a un altro incarico. Devono esserci sempre almeno due persone che conoscono il posto di stoccaggio e le procedure di codifica/decodifica oltre alle disposizioni su come e quando cambiare le chiavi. Queste procedure devono anche esigere che le chiavi siano cambiate immediatamente alla partenza di ogni dipendente che vi aveva accesso.

Chi è ***quello?***

L'esempio addotto in questo capitolo di un furbo artista della truffa che sfrutta il suo fascino per indurre il personale a condividere con lui le informazioni conferma l'importanza della verifica dell'identità. Anche la richiesta di farsi rispedire il codice sorgente a un sito FTP illustra l'importanza della conoscenza diretta del richiedente.

Nel ***Vademecum*** troverete le misure specifiche per verificare l'identità di un estraneo che richiede informazioni o domanda di fare qualcosa. Abbiamo parlato per tutto il libro della necessità di verifica. Nel ***Vademecum*** troverete i dettagli su come farlo.

Quarta parte

Innalzare la sbarra

15.

Presa di coscienza e training sulla sicurezza delle informazioni

Un ingegnere sociale è stato incaricato di rubarvi i piani del vostro nuovo prodotto innovativo che deve uscire tra due mesi. Che cosa può fermarlo?

Il vostro **firewall?** No.

Forti strumenti di autenticazione? No.

Sistemi di rilevamento delle intrusioni? No.

La cifratura? No.

Un accesso limitato ai numeri di telefono per gli accessi modem su linea commutata? No.

I nomi in codice ai server che rendono difficile a un esterno capire quale di loro ospita i progetti del prodotto? No.

La verità è che non esiste tecnologia al mondo che possa prevenire un attacco portato da un ingegnere sociale.

SICUREZZA GRAZIE A TECNOLOGIA, FORMAZIONE DELPERSONALEEPROCEDURE

Le ditte specializzate nell'esecuzione di "penetration test" riferiscono che i tentativi di intrusione nei sistemi informatici del cliente usando metodi di ingegneria sociale hanno successo quasi al cento percento. Le tecnologie di sicurezza possono rendere più difficili questi attacchi sottraendo il potere decisionale alle persone, però l'unica maniera efficace di ridurre la minaccia è nell'uso di tecnologie ***assieme*** a procedure che impongano regole base al comportamento del personale e a una preparazione e addestramento adeguati dei dipendenti.

C'è solo una maniera per tenere al sicuro i piani del prodotto ed è avere una forza lavoro preparata, consapevole e coscienziosa. Ciò significa un addestramento alle procedure ma

anche, e forse persino più importante, un programma di "awareness", di presa di coscienza sempre attivo. Alcune autorità del settore raccomandano che il quaranta percento del budget complessivo per la sicurezza dell'azienda sia investito sulla presa di coscienza.

Il primo passo consiste nel rendere tutti coloro che lavorano nella struttura consapevoli delle persone poco scrupolose che useranno l'inganno per manipolarli psicologicamente. I dipendenti devono essere consci delle informazioni da proteggere, e di come proteggerle. Una volta che capiscono meglio come possono essere manipolati, si trovano in una condizione migliore per accorgersi che è in corso un attacco.

La consapevolezza della sicurezza significa anche educare alle procedure aziendali di sicurezza. Come sarà esposto meglio successivamente, queste politiche presuppongono una serie di regole necessarie a guidare il comportamento del personale, affinché protegga i sistemi e le informazioni delicate.

Questo capitolo e il prossimo vi forniranno un programma di sicurezza che potrebbe salvarvi da attacchi costosi. Se non avete personale addestrato e attento che segua procedure mirate, non è questione di ***se*** ma di ***quando*** perderete informazioni preziose per mano di un ingegnere sociale. Non aspettate di essere colpiti da un attacco prima di mettere in vigore queste procedure: potrebbe essere devastante per la vostra impresa e per il benessere dei dipendenti.

CAPIRE COME GLI ATTACCANTI SI APPROFITTANO DELLA NATURA UMANA

Per sviluppare un positivo programma di training per prima cosa dovete capire come mai la gente è vulnerabile agli attacchi. Identificando queste tendenze nella fase di formazione (per esempio, focalizzando l'attenzione durante le discussioni in stile gioco di ruolo), potrete aiutare i vostri dipendenti a capire perché possiamo essere tutti manipolati dagli ingegneri sociali.

La manipolazione è stata studiata dai sociologi per almeno un cinquantennio. Robert B. Cialdini ha riassunto le sue ricerche sul numero del febbraio 2001 di "Scientific American", presentando le sei "tendenze base della natura umana" che vengono coinvolte in un tentativo di ottenere assenso a una richiesta.

Gli ingegneri sociali si basano su queste sei tendenze (in maniera consapevole o assai spesso inconscia) durante i loro tentativi di manipolazione.

Autorevolezza

La gente ha la tendenza a cedere quando una persona autorevole le fa una richiesta. Come discusso altrove in queste pagine, una persona può essere convinta a esaudire una richiesta se crede che il richiedente sia un'autorità o una persona autorizzata a fare una domanda del genere.

Nel suo libro *Influence,* il professor Cialdini riporta uno studio condotto in tre ospedali del Middle West in cui **ventidue** diverse guardiole sono state contattate da una persona che sosteneva di essere un medico dell'ospedale e dava istruzioni per somministrare un **farmaco** a un degente. Le infermiere che ricevevano queste istruzioni non conoscevano la persona che telefonava e non sapevano nemmeno se fosse un medico (non lo era). Inoltre, le istruzioni per il farmaco **arrivavano** per telefono, in chiara violazione della prassi ospedaliera. Il farmaco da somministrare non era autorizzato in corsia, e il **dosaggio** indicato era il doppio di quello massimo giornaliero, rischiando quindi di mettere a repentaglio la vita del paziente. Eppure Cialdini segnala che nel 95% dei casi "l'infermiera ha prelevato la dose indicata dall'armadietto medicinali e stava per somministrarla al paziente" prima di essere interrotta da un osservatore che le spiegava l'esperimento.

Esempi di attacco: Un ingegnere sociale tenta di indossare una maschera autorevole sostenendo di essere della divisione IT oppure un dirigente o uno stretto collaboratore di un dirigente dell'azienda.

Simpatia

La gente ha la tendenza a obbedire quando la persona che avanza la richiesta è riuscita a presentarsi accattivante o con interessi, fede e atteggiamenti simili a quelli della vittima.

Esempi di attacco: Conversando, l'attaccante riesce ad apprendere passatempi e interessi della vittima e dichiara simili interessi e passioni. Oppure può sostenere di venire dallo stesso stato o dalla stessa scuola, o di avere mete identiche nella vita. Inoltre l'ingegnere sociale tenterà di imitare il comportamento della vittima per creare una parvenza di somiglianza.

Ricambiare

Possiamo obbedire automaticamente a una richiesta quando ci è stato dato o promesso qualcosa di valore. Il dono può essere

un oggetto o un consiglio o un aiuto. Quando una persona ha fatto qualcosa per te, hai la tendenza a restituire, a ricambiare. Questa pulsione implacabile si presenta persino in situazioni in cui la persona che riceve il dono non l'aveva richiesto. Uno dei modi più efficaci per indurre le persone a farci un "favore" (obbedire a una richiesta) è fare un regalo o dare un aiuto che crei un obbligo implicito.

I membri della setta religiosa Hare Krishna sono sempre stati molto bravi a indurre la gente a donare alla loro causa regalando loro per primi un libro o un fiore. Se chi riceve cerca di restituire il dono, colui che l'ha regalato non lo accetta, spiegando che è un regalo per lui. Questo principio di restituzione è stato sfruttato dai Krishna per far aumentare in maniera sensibile le donazioni.

Esempi di attacco: Un dipendente riceve una telefonata da una persona che sostiene di essere del settore IT, questi gli spiega che alcuni computer aziendali sono stati infettati da un nuovo virus non riconosciuto dall'antivirus capace di distruggere tutti i file conservati su una macchina. Questa persona si offre di accompagnare il dipendente lungo la procedura per risolvere i problemi. Dopodiché chiede di provare una utility che è stata aggiornata di recente per permettere di cambiare password. Il dipendente è restio a dire di no perché l'altro gli ha appena regalato una teorica protezione da un virus, quindi ricambia obbedendo alla richiesta.

Coerenza

La gente ha la tendenza a dire di sì dopo aver sposato pubblicamente una causa. Una volta promesso che faremo una cosa, non vogliamo apparire inaffidabili o indesiderabili, così tenderemo a cercare di apparire coerenti con la nostra promessa o presa di posizione.

Esempio di attacco: L'attaccante si mette in contatto con una dipendente abbastanza novellina e le dà consigli sull'accordo da lei firmato di attenersi a certe procedure di sicurezza come precondizione per l'utilizzo dei sistemi informatici aziendali. Dopo avere discusso di alcune misure di sicurezza, colui che chiama chiede all'utente la sua password per "verificare l'ottemperanza" a queste politiche con la scelta di una password difficile. Una volta che lei ha rivelato la password, l'altro le consiglia di scegliere le prossime in modo che l'eventuale attaccante non riesca a indovinarle. La vittima obbedisce in base al suo desiderio di attenersi alle politiche aziendali e all'assunto che l'attaccante stia solo verificando la sua adesione.

Convalida sociale

Le persone hanno la tendenza a obbedire quando, in tal modo, sembrano allinearsi agli altri. Le azioni altrui sono accettate come convalida della correttezza del comportamento in questione.

Esempi **di** *attacco:* Colui che telefona sostiene di essere impegnato in uno studio e nomina altre persone dell'ufficio che a suo dire hanno già collaborato. La vittima, convinta che la collaborazione degli altri convalidi l'autenticità della richiesta, accetta di partecipare. Allora l'altro pone una serie di domande tra cui quelle che inducono la vittima a rivelare username e password.

Scarsità

La gente tende a dire di sì quando crede che l'oggetto cercato stia scarseggiando e altri siano in competizione per averlo, oppure che sia disponibile solo per un breve periodo di tempo.

Esempio di *attacco:* L'attaccante manda delle e-mail in cui sostiene che le prime cinquecento persone che si registreranno presso il nuovo sito web vinceranno i biglietti gratuiti per un nuovo film di successo. Quando un impiegato ignaro si registra presso il sito gli chiedono di fornire il suo indirizzo aziendale di e-mail e di scegliere una password. Tante persone tendono a usare per comodità la stessa password o una simile in ogni sistema informatico che usano. Sfruttando questo punto debole, l'attaccante tenterà in seguito di insidiare il lavoro del bersaglio e i suoi sistemi casalinghi sfruttando username e password inseriti durante la registrazione sul sito web.

CREARE PROGRAMMI DI ADDESTRAMENTO E PRESA DI COSCIENZA

Pubblicare un opuscolo sulla politica di sicurezza delle informazioni oppure dirigere il personale a una pagina intranet che la spiega non abbassa di per sé i rischi. Ogni impresa deve definire le regole per iscritto, ma anche fare sforzi speciali per indurre *tutti* coloro che lavorano con le informazioni aziendali o con i sistemi informatici a imparare e rispettare queste regole. Inoltre, dovete essere sicuri che tutti capiscano il senso di ogni strategia in modo da non aggirare le regole per pura comodità. Altrimenti l'ignoranza sarà sempre la pronta

scusa per il dipendente e l'esatto punto debole che gli ingegneri sociali sfrutteranno.

Il fine cruciale di ogni programma di presa di coscienza riguardo la sicurezza è di indurre il personale a cambiare comportamento, motivando ogni dipendente a ***voler*** partecipare alla protezione delle informazioni della struttura. In questo caso sarà molto motivante spiegare come la loro partecipazione regalerà un vantaggio non solo all'azienda ma anche allo stesso dipendente. Dato che l'azienda conserva certe informazioni personali su ogni lavoratore, quando i dipendenti fanno la loro parte per proteggere i dati o i sistemi d'informazione in realtà stanno proteggendo anche le loro.

Un programma di training alla sicurezza richiede un appoggio sostanzioso, le sue attività devono raggiungere qualsiasi persona abbia accesso a informazioni delicate o ai sistemi informatici, dev'essere continuo e regolarmente revisionato per aggiornare il personale sulle nuove minacce e punti deboli. I dipendenti devono comprendere che la direzione è totalmente impegnata nel programma, e dev'essere un impegno concreto, non un mero messaggio di auguri fatto con lo stampino. E il programma deve avere alle spalle risorse sufficienti per svilupparsi, comunicare, essere messo alla prova e misurarne il successo.

Scopi

La linea di condotta essenziale da tenere in mente nel preparare un programma di addestramento e presa di coscienza sulla sicurezza delle informazioni, è che esso deve imperniarsi sulla presa d'atto, in tutto il personale, che la sua azienda può essere attaccata in qualsiasi momento. Devono capire che ognuno di loro recita una parte nella difesa contro i tentativi di intrusione nei sistemi informatici o di furto di dati preziosi.

Visto che vari aspetti della sicurezza delle informazioni coinvolgono la tecnologia, è troppo facile per i dipendenti pensare che il problema possa essere risolto dai firewall e da altri strumenti di protezione. Lo scopo primario dell'addestramento dovrebbe essere quello di far nascere in ogni dipendente la consapevolezza di essere la prima linea della sicurezza complessiva dell'organizzazione.

L'addestramento deve avere uno scopo ben più alto del semplice impartire delle regole. Colui che progetta il programma deve prevedere la forte tendenza dei dipendenti, sempre sotto pressione perché completino il loro lavoro, a trascurare o ignorare le proprie responsabilità. È importante conoscere le tattiche dell'ingegneria sociale e sapere come difendersi dagli attac-

chi, ma i frutti arriveranno soltanto se il training sarà pensato in modo da concentrarsi soprattutto sulla ***motivazione*** nell'usare questo sapere.

L'azienda può affermare che il programma ha ottenuto il suo scopo minimo se tutti coloro che hanno completato la preparazione sono convinti e motivati da un unico concetto base: la sicurezza delle informazioni fa parte del loro impiego.

I dipendenti devono capire e accettare la realtà della minaccia degli ingegneri sociali, e che una grave perdita di informazioni segrete può mettere a repentaglio l'azienda oltre che le loro informazioni personali e il posto di lavoro. In un certo senso essere poco attenti alla sicurezza delle informazioni sul posto di lavoro equivale a essere superficiali con il proprio numero di carta di credito o PIN del Bancomat. Quest'ultimo potrebbe essere un paragone convincente per creare un certo interesse per questo genere di problematiche.

Mettere in atto il programma

Il responsabile del programma deve capire che non si tratta di un progetto a taglia unica, ma dev'essere allestito in modo da adattarsi alle necessità specifiche di gruppi diversi all'interno dell'impresa. Anche se tante politiche di sicurezza di cui si parlerà nel ***Vademecum*** valgono per tutto il personale, molte altre sono mirate. Come minimo, tante aziende avranno bisogno di programmi su misura per gruppi diversi come dirigenti, personale IT, informatici, personale non tecnico, segretari, centralinisti e custodi. (Vedi lo schema delle procedure secondo incarico nel ***Vademecum.)***

Dato che il personale della sorveglianza non dev'essere per forza esperto di computer e, a parte forse casi limitatissimi, non entra a contatto con queste macchine, di solito non viene considerato quando si progettano addestramenti del genere. Pero gli ingegneri sociali possono ingannare le guardie facendo in modo che permettano loro di entrare nello stabilimento o negli uffici, oppure convincendoli a fare un'azione che permette poi un'intrusione informatica. Per quanto i custodi non abbiano di sicuro bisogno dell'addestramento completo del personale che gestisce o usa i computer, ciò nonostante non devono essere trascurati nei programmi d'istruzione sui problemi della sicurezza.

Nel mondo delle imprese ci sono pochi argomenti su cui il personale dev'essere educato che siano tanto importanti e intrinsecamente tanto noiosi quanto la sicurezza. I programmi più intelligenti riescono a informare catturando nel contempo l'attenzione degli allievi e suscitando il loro entusiasmo.

Il programma dovrebbe essere un'esperienza interessante e interattiva, usando tecniche come le dimostrazioni dei metodi degli ingegneri sociali tramite i giochi di ruolo, la lettura degli articoli sui recenti attacchi ad altre imprese meno fortunate, la discussione su come avrebbero fatto gli allievi per prevenire il danno, oppure la visione di video divertenti e al contempo istruttivi. Ci sono varie compagnie specializzate che vendono questi video e i relativi materiali.

Gli aneddoti di questo libro vi forniscono molto materiale con cui spiegare metodi e tattiche dell'ingegneria sociale, per rendere consapevoli della minaccia e per dimostrare i punti deboli del comportamento umano. Mettete in conto di usare queste trame come base per giochi di ruolo. Inoltre, le storie proposte offrono spunti coloriti per awiare discussioni animate su come avrebbero potuto fare le vittime per impedire il successo dell'attacco.

Un astuto programmatore di corso e degli istruttori ingegnosi incontreranno molti problemi, ma escogiteranno anche tanti spunti per mantenere alta l'attenzione della classe e intanto motivare gli allievi a diventare parte della soluzione.

Struttura del training

Dovreste allestire un programma base di addestramento alla sicurezza che tutti i dipendenti devono frequentare. I nuovi assunti devono partecipare come parte dell'apprendistato iniziale. Raccomando inoltre che nessuno abbia accesso ai computer fino a quando non ha seguito una lezione base di orientamento sui problemi della sicurezza.

Per questa preparazione iniziale raccomando una lezione abbastanza tirata per non far calare l'attenzione e piuttosto breve, affinché i messaggi importanti non siano dimenticati. Se la quantità di materiale da affrontare giustifica sicuramente un addestramento più lungo, l'importanza di spiegare e motivare tramite un numero ragionevole di messaggi essenziali vince, a mio parere, qualsiasi strategia di lezioni lunghe una mezza giornata o una giornata intera tali da stordire la gente con eccessive informazioni.

In queste sedute bisogna insistere sul danno che può essere recato all'azienda e ai singoli dipendenti, a meno che tutto il personale non rispetti le buone abitudini di sicurezza. Ancor più importante che imparare le procedure specifiche è la motivazione dei dipendenti ad assumersi responsabilità personali nel campo della sicurezza.

Nelle situazioni in cui alcuni dipendenti non frequentano con

diligenza le lezioni, l'impresa dovrebbe pensare se sia il caso di usare altre forme didattiche, come video, lezioni al computer, corsi online o materiali scritti.

Dopo la breve lezione iniziale, dovrebbero essere previsti altri appuntamenti più lunghi per spiegare gli specifici punti deboli e le tecniche di attacco relative alla loro posizione nella struttura. E prevedete un aggiornamento all'anno come minimo. La natura della minaccia e i metodi usati per sfruttare la gente cambiano in continuazione, perciò il contenuto del programma dovrebbe essere sempre rinnovato. Inoltre, l'attenzione della gente cala con il tempo, quindi l'addestramento andrebbe ripetuto a intervalli ragionevoli per ribadire i principi base. Anche qui bisogna insistere affinché i dipendenti restino convinti dell'importanza delle misure di sicurezza e siano abbastanza motivati a rispettarle, e quindi non basta presentare le minacce specifiche e i metodi di ingegneria sociale.

I dirigenti devono concedere abbastanza tempo ai sottoposti perché si impratichiscano nelle procedure, e devono partecipare al programma. Non potete aspettarvi che il personale studi o segua le lezioni nel tempo libero. Ai nuovi assunti bisogna concedere tutto il tempo di prendere in esame le procedure di sicurezza e il materiale cartaceo prima di ricoprire l'incarico.

I dipendenti che cambiano posizione nell'organizzazione, passando a un incarico che contempla l'accesso al sistema informatico o a dati riservati, dovrebbero owiamente completare un programma di addestramento su misura per le loro nuove responsabilità. Per esempio, quando un operatore di computer diventa amministratore di sistema o un centralinista diventa segretario personale, dovrà sostenere un ulteriore training.

Contenuti dei corsi

Ridotti all'osso, tutti gli attacchi degli ingegneri sociali hanno lo stesso comune denominatore: l'inganno. La vittima è indotta a credere che l'attaccante sia un collega oppure una persona autorizzata all'accesso a informazioni riservate o a dare istruzioni contenenti azioni da eseguire al computer o su un macchinario correlato. Quasi tutti questi attacchi possono essere sventati se il dipendente preso di mira segue semplicemente due criteri:

- Verificare l'identità del richiedente. La persona che fa la richiesta è dawero chi sostiene di essere?

- Verificare se la persona è autorizzata. Ha diritto a sapere? È autorizzata ad avanzare questa richiesta?

Se le lezioni riescono a cambiare i comportamenti in modo che ogni dipendente diventi scmpoloso nel sottoporre a questi criteri ogni richiesta, il rischio degli attacchi degli ingegneri sociali si riduce in maniera proporzionale.

Un programma pratico che risolva i problemi del comportamento umano e dell'ingegneria sociale dovrebbe includere quanto segue:

- Una descrizione di come gli attaccanti sfruttano le capacità tipiche dell'ingegnere sociale per ingannare la gente.
- I metodi usati dagli ingegneri sociali per raggiungere l'obiettivo.
- Come riconoscere un presunto attacco di ingegneria sociale.
- La procedura per gestire le richieste sospette.
- Dove riferire i tentativi o gli attacchi andati a segno degli ingegneri sociali.
- L'importanza di indagare chiunque ponga una richiesta sospetta, indipendentemente dalla proclamata posizione o importanza di quella persona.
- Perché non ci si deve fidare implicitamente degli altri senza adatta verifica, anche se la tendenza sarebbe quella di concedere il beneficio del dubbio.
- L'importanza di verificare l'identità e la posizione di ogni persona che richiede informazioni o piaceri. (Vedi "Procedure di verifica e autorizzazione" nel ***Vademecum*** per i modi con cui verificare l'identità.)
- Procedure per proteggere le informazioni delicate, compresa la familiarità con i sistemi di classificazione dei dati.
- L'ubicazione delle procedure di sicurezza dell'organizzazione e la loro importanza per la protezione delle informazioni e dei sistemi di informazione.
- Un sommario delle politiche chiave e una spiegazione del loro significato. Per esempio, dovete insegnare a ogni dipendente come escogitare una password difficile da indovinare.
- L'obbligo per tutto il personale di obbedire a queste procedure e le conseguenze del non rispettarle.

Per definizione l'ingegneria sociale prevede una qualche specie di interazione umana. Un attaccante userà spesso una notevole varietà di metodi e tecnologie della comunicazione per arrivare allo scopo. Perciò un programma completo di presa di coscienza cercherà di includere parte di quanto segue:

- Procedure di sicurezza relative alle password nei computer e nelle caselle vocali.
- Procedure per quando occorre rivelare informazioni o materiali delicati.
- Politica dell'uso della posta elettronica, comprese le misure per prevenire attacchi tipo virus, worm e cavalli di Troia.
- Esigenze fisiche di protezione come i tesserini da esibire.
- La responsabilità di bloccare le persone presenti nei locali che non mostrino il tesserino di riconoscimento.
- Le migliori pratiche sicure dell'uso della segreteria telefonica e delle caselle vocali.
- Come decidere il livello di segretezza delle informazioni, e le migliori misure per proteggere le informazioni sensibili.
- Come cestinare nel modo corretto i documenti e i supporti informatici che contengono o hanno contenuto materiali riservati.

Inoltre, se l'azienda prevede di svolgere dei penetration test per valutare l'efficacia delle difese contro gli attacchi degli ingegneri sociali, bisognerebbe preavvertire i dipendenti. Che sappiano pure che in un momento qualsiasi potrebbero ricevere una telefonata o altre comunicazioni che utilizzeranno le tecniche degli attaccanti, in quanto parte dell'esame. Usate i risultati di questi test non per punire ma per valutare la necessità di ulteriore addestramento in questi settori.

I dettagli su tutte queste voci li troverete nel ***Vademecum.***

METTERE **ALLA PROVA**

La vostra azienda potrebbe voler mettere alla prova il personale per verificare l'assimilazione delle informazioni proposte durante l'addestramento alla sicurezza prima di porlo davanti a un computer. Se prevedete test in rete, ci sono molti programmi di assessment design che vi permetteranno di analizzare immediatamente i risultati dei test per capire quali parti debbano essere spiegate meglio.

Inoltre la vostra impresa può prendere in esame la possibilità di fornire un certificato, come testimonianza del completamento della preparazione, quale ricompensa e motivazione.

In quanto elemento di routine del programma completato, raccomandiamo di richiedere a ogni dipendente di firmare un'impegnativa sulle politiche e principi di sicurezza insegnati nel programma. Alcune ricerche indicano che una persona che

si impegna, firmando un accordo di questo tipo, ha maggiori stimoli e attenzioni nell'attenersi alle procedure.

PRESA DI COSCIENZA SENZA SOLUZIONI DI CONTINUITÀ

Quasi tutti sanno che quanto si apprende, anche in campi importanti, tende a svanire a meno di non essere rinfrescato periodicamente. Data l'importanza della consapevolezza dei dipendenti riguardo l'argomento della difesa dagli attacchi degli ingegneri sociali, è essenziale prevedere un programma di attenzione continua.

Un metodo per tenere la sicurezza sempre a mente nel lavoratore è di renderla uno specifico incarico di ogni persona dell'organizzazione. In questo modo li incoraggerete a riconoscere il ruolo svolto all'interno della sicurezza complessiva dell'azienda. Altrimenti, vi troverete di fronte a un atteggiamento rispetto alla sicurezza del tipo "non è roba che mi riguarda".

Benché la responsabilità complessiva di un programma sulla sicurezza delle informazioni sia di solito affidata a una persona della sorveglianza o del settore Information Technology, lo sviluppo di un programma di attenzione sarà probabilmente migliore qualora sia impostato in modo congiunto con il settore preposto alla formazione generale.

Il programma continuativo di consapevolezza dev'essere creativo e utilizzare ogni canale disponibile per comunicare i messaggi sulla sicurezza in maniera da non farli dimenticare, affinché il personale sia sempre tenuto vigile alle buone abitudini. Come per la pubblicità classica, umorismo e intelligenza non guastano. Variare la stesura dei messaggi impedisce che diventino tanto risaputi da essere ignorati.

L'elenco delle possibilità per un programma continuativo di presa di coscienza potrebbe contemplare:

- Fornire copie di questo libro a tutti i dipendenti.
- Inserire materiali informativi nella newsletter aziendale: articoli, promemoria nei boxini (preferibilmente brevi e che calamitino l'attenzione) oppure fumetti, tanto per fare qualche esempio.
- Appendere un'immagine dell'impiegato del mese per la sicurezza.
- Affiggere manifesti nelle aree del personale.
- Attaccare avvisi in bacheca.
- Fornire allegati stampati alla busta paga.

- Mandare aggiornamenti per posta elettronica.
- Usare salvaschermo che parlino della sicurezza.
- Trasmettere un annuncio che parli della sicurezza nel sistema di caselle vocali.
- Stampare adesivi per i telefoni con messaggi del tipo "La persona con cui stai parlando è davvero chi dice di essere?".
- Preparare promemoria da far comparire sul computer dopo il logon, tipo: "Se stai inviando informazioni riservate in e-mail, codificale".
- Inserire l'attenzione alla sicurezza come voce immancabile nei rapporti annuali sulle prestazioni del dipendente.
- Fornire promemoria attinenti in intranet, casomai usando fumetti o storielline divertenti e comunque incentivando l'interesse dei dipendenti a leggerli.
- Piazzare in mensa uno schermo per messaggi elettronici su cui passano messaggi sulla sicurezza che cambiano di continuo.
- Distribuire volantini o opuscoli.
- E pensate anche a trovate come i biscotti della fortuna in mensa, ciascuno contenente al posto dell'oroscopo un messaggio sulla sicurezza.

La minaccia è costante. Anche i vostri messaggi devono essere costanti.

COS'HO DA GUADAGNARE?

Oltre a questi programmi raccomando fortemente uno schema attivo e ben propagandato di incentivi. Dovete premiare i dipendenti che hanno individuato e prevenuto un tentato attacco oppure hanno contribuito in qualche altra maniera al successo del programma. L'esistenza di ricompense dovrebbe essere ricordata ai dipendenti durante tutte le lezioni sulla sicurezza, e le infrazioni dovrebbero essere ampiamente pubblicizzate in tutta l'organizzazione.

L'altra faccia della moneta è far capire alla gente le conseguenze delle infrazioni alle politiche di sicurezza, sia per riottosità sia per negligenza. Anche se tutti commettiamo errori, le ripetute violazioni alle procedure non devono essere tollerate.

Vademecum per la sicurezza delle informazioni aziendali

Nove grandi aziende ed enti statali su dieci sono stati attaccati dagli intrusi informatici, stando ai risultati di uno studio condotto dall'FBI e riferiti dall'Associated Press nell'aprile del 2002. Dato interessante, la ricerca ha riscontrato che solo un'azienda su tre ha riportato o reso pubblico un attacco. Questa reticenza a svelare i danni è giustificabile. Per evitare di perdere la fiducia dei clienti e prevenire ulteriori attacchi da parte di intrusi che hanno scoperto la vulnerabilità di una compagnia, quasi tutte le strutture non rendono pubblici gli incidenti ai danni della sicurezza informatica.

Sembra che non ci siano statistiche sugli attacchi degli ingegneri sociali. e anche se ci fossero i numeri sarebbero altamente inaffidabili. In quasi tutti i casi, un'azienda non si accorge che un ingegnere sociale ha 'rubato" le informazioni, quindi tanti attacchi passano ignorati o non sono divulgati.

Potete mettere in atto contromisure efficaci contro quasi tutti i tipi di attacco di ingegneri sociali. Però guardiamo in faccia la realtà: a meno che tutti nell'organizzazione capiscano l'importanza della sicurezza e si impegnino a conoscere e rispettare le procedure aziendali relative, gli attacchi degli ingegneri sociali rappresenteranno sempre un grave rischio.

Infatti, man mano che facciamo passi avanti quanto ad armi tecnologiche contro le falle nella sicurezza. le tattiche di inganno usate dagli ingegneri sociali per attingere a informazioni proprietarie o per penetrare la rete aziendale diventeranno di sicuro molto piu frequenti e sofisticate. Una spia industriale tenterà naturalmente $ arrivare allo scopo usando il metodo più facile e che contempla meno rischi di essere individuato. Nella pratica, un'azienda che ha protetto la sua rete e i sistemi informatici usando tecnologie all'ultimo grido può essere più vulnerabile agli attaccanti che sfruttano le strategie, tattiche e metodi dell'ingegneria sociale per ottenere quel che vogliono.

Questo capitolo presenta dettagliate politiche studiate per minimizzare i rischi degli attacchi da parte di ingegneri sociali, una serie di misure contro i tentativi che non si basino strettamente sullo sfruttamento dei punti deboli tecnologici, ma usino qualche pretesto o trucco per ingannare un impiegato fidato affinché fornisca informazioni o esegua azioni che daranno al malfattore accesso a delicate informazioni di lavoro o alle reti e sistemi informatici dell'azienda.

Le politiche della sicurezza sono composte da una serie di chiare istruzioni che forniscono le linee di condotta per il comportamento dei dipendenti per la protezione delle informazioni, e sono un mattone fondamentale per allestire controlli efficaci per controbattere i potenziali attacchi alla sicurezza. Queste procedure sono ancora più significative quando si tratta di prevenire e individuare gli attacchi degli ingegneri sociali.

I controlli efficaci sono implementati addestrando i dipendenti tramite procedure ben documentate. Tuttavia, è importante ricordare che le politiche di sicurezza, anche se seguite con fervore religioso dal personale, non danno la garanzia assoluta di poter sventare qualsiasi attacco. Una meta ragionevole rimane quella di abbassare i rischi a livelli accettabili.

Le procedure presentate in queste pagine comprendono anche misure che hanno ragione di comparire, per quanto non siano centrate su temi di ingegneria sociale, perché trattano tecniche usate normalmente negli attacchi. Per esempio, i consigli su come aprire gli attachment, che potrebbero installare subdoli cavalli di Troia, i quali permetterebbero all'attaccante di impossessarsi del computer della vittima, sono pertinenti a un metodo usato spesso dagli intrusi informatici.

I passi per approntare un programma

Un programma completo di sicurezza delle informazioni inizia di solito con la valutazione del rischio intesa a decidere:

- Quali informazioni devono essere protette?
- Quali sono le minacce specifiche contro questi beni?
- Quale può essere il danno all'impresa qualora si concretizzassero queste minacce potenziali?

La prima meta della valutazione del rischio è stilare una scaletta di priorità delle informazioni che necessitano di salvaguardie immediate, quindi decidere se queste contromisure possano essere positive in un'analisi costi-benefici. In parole povere, quali beni bisogna proteggere per primi e quanti soldi spendere per proteggerli?

È essenziale che la direzione sostenga con forza la necessità di sviluppare misure di sicurezza e un relativo programma di formazione. Come per qualsiasi altro programma aziendale, se quello sulla sicurezza vuole avere successo la direzione deve fare molto di più che limitarsi a garantire il suo appoggio, deve dimostrare un vero impegno con l'esempio diretto. I dipendenti devono sapere che la direzione crede sul serio che la sicurezza delle informazioni sia essenziale alle operazioni, che proteggere le informazioni è fondamentale perché la compagnia rimanga in piedi e che ogni posto di lavoro può dipendere dal successo di questo programma.

La persona incaricata di stilare le procedure di sicurezza delle informazioni deve anche capire che esse devono essere scritte in una forma scevra di tecnicismi, facilmente comprensibile per i dipendenti meno tecnologizzati. È anche importante che il documento chiarisca perché ogni misura è importante, altrimenti il dipendente potrebbe snobbarle

come pura perdita di tempo. L'estensore dovrebbe creare un documento per presentare la politica complessiva e un altro separato per le varie misure singole, visto che la politica cambierà meno di frequente delle specifiche misure messe in atto per rispettarla.

Inoltre, l'estensore dovrebbe sapere come usare le *tecnologie* per la sicurezza per far rispettare le procedure valide. Per esempio, quasi tutti i sistemi operativi rendono possibile esigere che la password si conformi a certe specifiche come la lunghezza. In alcune aziende, la proibizione di scaricare programmi può essere controllata tramite impostazioni locali o globali all'interno dei sistemi operativi. Le varie procedure dovrebbero richiedere l'uso della tecnologia per la sicurezza ogni volta che fa risparmiare eliminando i processi decisionali basati sulle persone.

I dipendenti devono essere informati dei danni derivanti dal non uniformarsi alle politiche e alle procedure di sicurezza. Bisogna prevedere e pubblicizzare ampiamente un insieme di contromisure per chi viola la sicurezza. Inoltre, andrebbe creato un programma di ricompense per i dipendenti che dimostrano di rispettare attentamente queste misure o che individuano e riportano un problema al sistema. Ogni volta che ricompensate un dipendente per aver sventato una falla alla sicurezza, il fatto dev'essere pubblicizzato in tutta la struttura, per esempio con un articolo sulla newsletter.

Una meta del programma di presa di coscienza sarebbe quella di far capire l'importanza delle misure decise e il danno che può risultare dall'incapacità a seguire queste regole. Data la natura umana, ogni tanto il personale ignorerà o aggirerà i prowedimenti che gli sembrano ingiustificati o troppo laboriosi. È responsabilità della direzione verificare che il personale comprenda l'importanza di questa politica e sia motivato a rispettarla piuttosto che trattarla come una serie di ostacoli da aggirare.

È importante ricordare che la politica sulla sicurezza delle informazioni non può essere scolpita nel marmo. Con il mutare dei metodi commerciali e la diffusione di nuovi strumenti per la sorveglianza, queste misure dovranno essere modificate o arricchite. Prevedete una scaletta regolare di revisioni e aggiornamenti. Le procedure aziendali devono essere reperibili nell'intranet aziendale oppure in una cartella a disposizione di tutti. In questo modo aumentano le probabilità che siano revisionate di frequente e garantirete ai dipendenti un metodo comodo per trovare velocemente la risposta alle domande relative.

Per finire, bisognerebbe organizzare periodici penetration test e vulnerability assessment tramite metodi e tattiche di ingegneria sociale per far uscire allo scoperto le debolezze nella formazione o nell'aderenza alle procedure aziendali. Prima di usare qualsiasi metodo per saggiare la penetrabilità, dovrete informare il personale che, di tanto in tanto, possono essere messi in atto test del genere.

Come usare questa politica

La politica dettagliata presentata in questo capitolo è solo un sottogruppo delle politiche sulla sicurezza delle informazioni, secondo me, necessarie per minimizzare i rischi. Quindi non dovrebbe essere considerata una lista completa sulla sicurezza delle informazioni. Piuttosto

è la base su cui costruire un esaustivo corpo di politiche di sicurezza adatto alle necessità specifiche della vostra azienda.

Gli estensori dovranno scegliere le misure adatte all'ambiente specifico della loro azienda e alle sue mete commerciali. Ogni struttura, avendo diverse necessità di sicurezza in base alle strategie commerciali, agli obblighi legali, alla cultura aziendale e ai sistemi di informazione usati, prenderà ciò che le serve da quanto è qui presentato e lascerà perdere il resto.

Bisogna anche fare delle scelte su quanto devono essere stringenti le misure in ogni categoria. Una piccola azienda in un piccolo stabilimento in cui quasi tutti i dipendenti si conoscono non dev'essere molto preoccupata per gli attacchi telefonici attuati fingendosi uno del personale (anche se ovviamente l'impostore può spacciarsi come un fornitore). Inoltre, nonostante i rischi maggiori, un'azienda strutturata attorno a una cultura più disinvolta e rilassata desidererà adottare soltanto un sottogruppo limitato delle politiche qui raccomandate per conseguire i propri obiettivi di sicurezza.

CLASSIFICAZIONE DEI DATI

Una politica sulla classificazione dei dati, cioè la loro etichettatura e segretazione, è fondamentale per proteggere le informazioni dell'organizzazione, allestendo una serie di classi ver gestire il rilascio di dati sensibili. Questa politica fornisce un quadro d'insieme per proteggere le informazioni aziendali rendendo consapevoli tutti i dipendenti del livello di riservatezza di qualsiasi dato.

Se operate senza un criterio di classificazione dei dati, situazione corrente in quasi tutte le aziende odierne, lasciate quasi tutte le decisioni nelle mani dei singoli lavoratori. Naturalmente le decisioni dei dipendenti sono di solito basate su fattori soggettivi piuttosto che sull'informazione stessa. sulla sua delicatezza, crucialità e valore. Inoltre, i dati trapelano all'esterno perché il personale ignora l'eventualità che rispondendo a una richiesta l'informazione possa finire nelle mani di un malintenzionato.

La politica di classificazione dei dati predispone linee guida per gestire a vari livelli di riservatezza le informazioni di valore. Quando a ogni voce è assegnata una valutazione della riservatezza, il personale può seguire una serie di procedure per la gestione dei dati proteggendo così l'azienda dalla rivelazione inconsapevole o negligente di informazioni preziose. Queste procedure riducono la possibilità che i dipendenti vengano ingannati in modo da fornire informazioni "sensibili" a persone non autorizzate.

Ogni dipendente dev'essere addestrato riguardo a questa politica, compresi coloro che di solito non usano i computer o i sistemi di comunicazione. Dato che ogni membro della forza lavoro, compreso il personale delle pulizie, i custodi e gli addetti alle fotocopie, oltre ai consulenti, gli incaricati e persino gli awentizi, può avere accesso alle informazioni delicate, tutti possono essere bersaglio di un attacco.

La dirigenza deve decidere un ***detentore informazioni*** responsabile di tutti i dati utilizzati attualmente nell'azienda. Tra le varie cose, questa figura sarà responsabile della protezione delle informazioni. Di regola, deciderà il livello di classificazione da assegnare in base alla necessità

di proteggere i dati, rivedrà periodicamente il livello di classificazione assegnato e deciderà possibili interventi correttivi. Il detentore informazioni potrà anche delegare la responsabilità della protezione dei dati a un ***custode.***

Categorie e definizioni della classificazione

I fornitori dovrebbero essere suddivise secondo diversi livelli di riservatezza in base alla loro delicatezza. Una volta istituito un particolare sistema, sarà laborioso e costoso riorganizzare le informazioni secondo nuove categorie. Nel nostro esempio ho scelto quattro livelli, adatti a quasi tutte le aziende medie e grandi. A seconda del numero e genere delle informazioni delicate, l'azienda può decidere di aggiungere altre categorie introducendo modalità specifiche di controllo delle informazioni. Nelle piccole aziende potrà bastare uno schema a tre livelli. Ricordate che più complesso è lo schema più costa all'organizzazione formare il personale e attuare il sistema.

Confidenziali

Questa categoria di informazioni è la più delicata. Le informazioni confidenziali sono da usare soltanto dentro la struttura. In quasi tutte le occasioni devono essere condivise solo da un numero limitatissimo di persone con incontestabile diritto a essere informate. La natura delle informazioni confidenziali è tale che qualsiasi diffusione non autorizzata potrebbe danneggiare gravemente l'azienda, gli azionisti, i partner e/o i clienti. Di solito ricadono in una di queste categorie:

- Informazioni su segreti commerciali, codice sorgente proprietario, specifiche tecniche o funzionali o dati sul prodotto che potrebbero avvantaggiare la concorrenza.
- Informazioni di marketing o finanziarie non aperte al pubblico.
- Qualsiasi altra informazione cruciale per le operazioni come le future strategie commerciali.

Personali

Questa categoria copre le informazioni di natura personale da utilizzare soltanto entro la struttura. Qualsiasi diffusione non autorizzata di informazioni personali potrebbe danneggiare gravemente i dipendenti o l'azienda qualora cadessero in mano a figure non autorizzate (soprattutto gli ingegneri sociali). Le informazioni personali dovrebbero comprendere la cartella medica del dipendente, le assicurazioni sanitarie, le informazioni sui conti bancari, lo stipendio e ogni dato personale non di pubblico dominio.

Le "informazioni a uso interno" sono spesso definite "sensibili" dal personale addetto alla sicurezza. Ho scelto "interno" perché spiega meglio a quale pubblico si rivolge la categoria. Uso il termine "sensibile" (sensitive) non in quanto categoria di classificazione, ma come comodo metodo per riferirmi alle informazioni non pubbliche.

Interne

Questa categoria di informazioni può essere fornita liberamente a ogni persona dell'organizzazione. Di regola, la rivelazione non autorizzata di informazioni a uso interno non dovrebbe causare grave nocumento all'azienda, agli azionisti, ai partner, ai clienti o ai dipendenti. Tuttavia, gli esperti di ingegneria sociale possono usarle per camuffarsi da dipendente autorizzato, incaricato esterno o fornitore per ingannare il personale ignaro affinché fornisca informazioni utili all'accesso non autorizzato ai sistemi informatici della struttura.

Bisogna firmare un accordo di riservatezza prima di rivelare informazioni a uso interno a terzi come i dipendenti delle ditte fornitrici, incaricate di un servizio, consociate ecc. Di solito le informazioni interne comprendono tutto quanto viene usato nell'attività giornaliera che non dovrebbe essere rivelato a esterni, come l'organigramma, i numeri di modem della rete. i nomi dei sistemi interni, le procedure di accesso remoto, i codici degli uffici spese ecc.

Pubbliche

Informazioni pensate apposta per essere diffuse pubblicamente. Possono essere date liberamente a chiunque, come i comunicati stampa, le informazioni sulle persone da contattare all'assistenza ai clienti oppure gli opuscoli dei prodotti. Va notato che ogni informazione non etichettata esplicitamente come pubblica dovrebbe essere ritenuta sensibile.

Terminologia dei dati classificati

In base alla sua classificazione, un dato dovrebbe essere distribuito a determinate categorie di persone. Molte politiche di questo capitolo fanno riferimento a informazioni date a *persona non verificata.* Per i fini di queste politiche, una persona non verificata è colui che il dipendente non conosce direttamente come collega con un incarico che gli consenta accesso alle informazioni o che non è stato garantito da terzi fidati.

Sempre per i fini di queste politiche, una *persona fidata* è conosciuta direttamente ed è nota come dipendente, cliente o consulente dell'azienda, con un incarico che l'autorizza ad accedere alle informazioni. Una persona fidata può anche essere un dipendente di un'azienda che ha un rapporto duraturo con la vostra (per esempio un cliente, un fornitore o una consociata che ha firmato un contratto di riservatezza).

In una *garanzia da parte di terzi,* una persona fidata garantisce sull'incarico o status di una persona e sul diritto a pretendere informazioni o azioni. Ricordate che in certi casi queste procedure vi richiedono di verificare che la persona fidata sia ancora alle dipendenze della ditta, prima di rispondere alla richiesta di informazioni o azioni da parte di qualcuno garantito da lei.

Un *account privilegiato* è un account informatico o altro che ha diritti di accesso che va oltre il normale account utente, per esempio quello di amministratore di sistema. I dipendenti con account privilegiati

hanno di solito la possibilità di modificare i privilegi utente o di eseguire funzioni di sistema.

Una *casella vocale generica* di dipartimento è una mailbox vocale o segreteria telefonica cui risponde un messaggio generico del settore. Viene usata per proteggere i nomi e gli interni dei dipendenti che lavorano in un dato ufficio.

PROCEDURE DI VERIFICA E AUTORIZZAZIONE

I ladri di informazioni usano di solito tattiche ingannevoli per ottenere o accedere a informazioni commerciali confidenziali, facendosi passare per legittimi dipendenti, incaricati o partner. Per mantenere una sicurezza efficace, un dipendente che riceve una richiesta di eseguire un'azione o di rivelare informazioni sensibili deve identificare con sicurezza chi chiama e la sua posizione prima di acconsentire.

Le procedure raccomandate fornite in questo capitolo sono pensate per aiutare il dipendente che riceve una domanda tramite telefono, e-mail o fax a decidere se la richiesta e la persona che la inoltra siano legittime.

Richieste da persona fidata

Una richiesta di informazioni o azioni da parte di persona fidata può esigere:

- Una verifica che l'azienda impieghi o abbia rapporti tali con la persona da giustificare l'accesso a tale categoria di informazioni. Questo per impedire che ex dipendenti, fornitori, incaricati esterni e altri non più associati all'azienda si spaccino come personale attivo.
- Una verifica che la persona abbia diritto di sapere e sia autorizzata ad avere accesso alle informazioni o a richiedere un'azione.

Richieste da persona non accertata

Quando una richiesta proviene da una persona non accertata, subentra una ragionevole procedura di verifica per identificare con sicurezza la persona richiedente quale autorizzata a ricevere le informazioni, soprattutto quando ciò coinvolge in qualche modo computer o macchinari correlati. Questa procedura è il controllo fondamentale per sventare gli attacchi degli ingegneri sociali: se simili procedure di verifica sono rispettate, ridurranno in maniera spettacolare gli attacchi riusciti.

E importante che non rendiate così gravoso questo processo da diventare troppo costoso o essere ignorato dal personale.

Come precisato sotto, la procedura di verifica prevede tre passi:

- Verificare che la persona sia effettivamente chi sostiene di essere.
- Verificare che il richiedente sia attualmente un dipendente oppure abbia un rapporto con l'azienda che l'autorizza ad accedere.

- Decidere che la persona è autorizzata a ricevere l'informazione specifica o a richiedere quella data azione.

Primo passo: verifica dell'identità

I passi raccomandati per la verifica sono elencati di seguito in ordine di efficacia. Più alto il numero, più efficace il metodo. Inoltre a ogni voce è allegata una valutazione delle debolezze di quel particolare metodo, oltre ai modi in cui l'ingegnere sociale può sconfiggere o aggirare la misura al fine di ingannare un dipendente.

Identificazione di chiamata (presumendo che questa opzione sia prevista nella rete telefonica aziendale). Accertatevi sullo schermo se la telefonata provenga dall'interno o dall'esterno, e che il nome o numero di telefono corrisponda all'identità fornita da chi chiama.
Debolezza: l'informazione sulle chiamate esterne può essere falsificata da chi ha accesso a un PBX o a un centralino collegato al servizio di telefonia digitale.

Richiamare. Cercatelo nell'elenco aziendale e richiamatelo presso l'interno per verificare che sia un membro del personale.
Debolezza: un attaccante competente può trasferire la chiamata a un interno aziendale in modo che, quando si fa la telefonata di verifica al numero comparso nell'elenco, essa venga rimbalzata al numero esterno dell'attaccante.

Garanzie. Una persona fidata garantisce l'identità del richiedente.
Debolezza: gli attaccanti riescono spesso con qualche pretesto a convincere un altro dipendente della propria identità di modo che questi garantisca per loro.

Segreto condiviso. Usate un segreto aziendale, come una password o un codice giornaliero.
Debolezza: se ne sono a conoscenza molte persone, è facile che lo sia anche l'attaccante.

Supervisore/capoufficio. Telefonate al superiore del dipendente per verificare.
Debolezza: se il richiedente ha fornito il numero per telefonare al suo capoufficio, la persona che il dipendente contatta quando chiama potrebbe non essere il vero capoufficio bensì un complice.

E-mail sicure. Richiedete un messaggio con firma digitale.
Debolezza: se un attaccante ha già compromesso un computer e installato un Key logger* per rubare la pass phrase, può inviare anche una e-mail con firma elettronica che sembri provenire dal dipendente.

Riconoscimento vocale. La persona che riceve la richiesta ha già trattato con il richiedente (preferibilmente di persona), sa per certo che è

*** È un software che registra i caratteri digitali sulla tastiera, e opzionalmente li invia all'estemo via Internet. *[N.d.R.]***

una persona fidata e la conosce abbastanza da identificare la sua voce per telefono.

Debolezza: è un metodo abbastanza sicuro, difficile da aggirare per l'attaccante, ma non serve se la persona interpellata non ha mai visto o sentito il richiedente.

Soluzione password dinamica. Il richiedente si autentica usando una password dinamica come un Secure ID.

Debolezza: per battere questo metodo un attaccante deve procurarsi un apparecchio di password dinamica oltre al PIN del dipendente cui appartiene legittimamente, oppure deve convincerlo a leggere l'informazione sullo schermo e fornirgli il PIN.

***In carne** e ossa con il documento d'identità. Il* richiedente si presenta di persona e fornisce un tesserino o un altro documento d'identità, possibilimente con la foto.

Debolezza: spesso gli attaccanti riescono a rubare un tesserino o a crearne uno che sembri autentico, però di solito evitano questa tattica perché apparire di persona comporta il rischio di essere identificato e denunciato.

Secondo passo: verifica dello status del dipendente

La massima minaccia alla sicurezza delle informazioni non proviene dall'ingegnere sociale professionista né dall'intruso informatico dotato, ma da qualcuno molto più vicino: il dipendente appena licenziato desideroso di vendicarsi oppure di mettere su un'impresa sfruttando i dati rubati dall'azienda. (Ricordate che una variante di questa procedura può anche essere usata per verificare che qualcuno abbia ancora una relazione d'affari con la vostra azienda, tipo fornitore, servizio esterno incaricato *o* a contratto.)

Prima di procurare informazioni delicate a un'altra persona o di accettare istruzioni per fare qualcosa sul computer o apparecchi correlati, verificate sempre che il richiedente faccia ancora parte dell'organigramma aziendale usando uno di questi metodi.

Elenco del personale. Se l'azienda ha un elenco online che riporta con esattezza i dipendenti attivi, accertare che il richiedente vi figuri ancora.

Verifica da parte del superiore del richiedente. Chiamate il suo superiore usando il numero che compare nell'elenco. non auello fornito dal richiedente.

Verifica nel settore o ufficio del richiedente. Chiamate il settore o ufficio del richiedente e domandate se faccia ancora parte del personale.

Terzo passo: verifica dell'autorizzazione ad accedere

Oltre a verificare che il richiedente appartenga ancora al personale o abbia un rapporto di lavoro con la vostra azienda, resta ancora il problema se sia autorizzato ad avere accesso alle informazioni richieste o sia autorizzato a pretendere specifiche azioni che possano coinvolgere computer o apparecchi correlati.

Questa decisione può essere presa usando uno dei metodi seguenti.

Consultare elenchi di incarico/gruppo/responsabilità. Un'azienda può fornire un tempestivo accesso alle autorizzazioni stampando elenchi dei dipendenti aventi diritto alle date informazioni. Questi elenchi possono essere strutturati secondo incarico, ufficio o settore, responsabilità o tramite una combinazione dei tre, e dovrebbero essere conservati in rete per essere aggiornati e procurare un veloce accesso all'autorizzazione. Di solito i detentori di informazioni sono responsabili della creazione e conservazione delle liste di accesso alle informazioni sottoposte al loro controllo.

en l' da un capoufficio.] p ente n il superiore o capoufficio del ric affinché lo autorizzi a ›l alla richiesta.

Ottenere l'autorizzazione dal detentore di informazioni o da un suo delegato. Il detentore delle informazioni è il giudice ultimo per decidere se sia il caso di garantire l'accesso a una data persona. La procedura del controllo dell'accesso informatico significa che il dipendente deve contattare il superiore immediato perché approvi la richiesta di accesso in base all'incarico ricoperto. Se non esiste una definizione di auesto incarico, è responsabilità del capoufficio contattare il relativo detentore di informazioni affinché dia il permesso. Questa catena di comando dovrebbe essere rispettata in modo che i detentori di informazioni non siano gravati da troppe richieste.

Ottenere l'autorizzazione tramite pacchetto software proprietario. Per le grandi aziende in un settore altamente competitivo, sarebbe consigliabile allestire un pacchetto software proprietario che fornisca le autorizzazioni. Gli utenti non potrebbero controllare i diritti all'accesso degli altri, ma inserirebbero il nome e l'identificatore associato indicando le informazioni richieste. Il programma fornirà una risposta indicante l'autorizzazione all'accesso del dipendente a queste informazioni. Tale alternativa evita il pericolo di creare un elenco del personale, con i rispettivi diritti d'accesso a informazioni preziose, critiche o delicate, che può essere rubato.

POLITICHE GESTIONALI

È importante ricordare che queste liste sono un gentile invito per gli ingegneri sociali. Pensateci un attimo: se un attaccante che sta prendendo di mira una compagnia si accorge che questa conserva elenchi del genere farà di tutto per ottenerli, e una volta avuti fra le mani, essi gli apriranno molte porte mettendo l'azienda in una condizione di grave pericolo.

Le seguenti politiche riguardano i dipendenti a livello dirigenziale, e sono suddivise in classificazione dati, diffusione delle .informazioni, gestione dei telefoni e politiche miscellanee. Ricordo che ogni categoria utilizza una sua struttura di numerazione per la facile identificazione delle misure individuali.

Politiche riguardanti la classificazione dei dati

Per classificazionedati si intende il modo in cui la vostra azienda ordina in classi la sensibilità delle informazioni e quanti dovrebbero avervi accesso.

Assegnare una classificazione ai dati .

Politica: tutte le informazioni di valore, cruciali o sensibili pertinenti al lavoro devono avere una categoria di classificazione assegnata dal detentore di informazioni designato o da un suo delegato.

Spiegazione/Note: il detentore designato, o il delegato, assegnerà una classificazione consona a qualsiasi informazione usata di norma per arrivare a una meta commerciale. Inoltre, controllerà chi può accedere a quell'informazione e quale uso può farne. Il detentore può cambiare la classificazionee indicare un periodo di tempo per la desegretazione automatica.

Qualsiasi voce non contrassegnata in modo diverso dovrebbe essere classificata come *sensibile.*

Diffondere le procedure di gestione delle informazioni classificate

Politica: l'azienda deve prevedere procedure che governino la diffusione delle informazioni in ogni categoria.

Spiegazione/Note: una volta effettuate le classificazioni, occorrono procedure per la diffusione delle informazioni al personale e agli esterni come evidenziato nelle procedure di verifica e autorizzazione già esposte in questo capitolo.

Etichettare tutte le voci

ic contrassegnare chiaramente a i a stampati sia i supporti :hivi contenenti informazioni confidenziali, personali o interne in modo che appaia evidente la corretta classificazione dei dati.

Spiegazione/Note: i documenti su carta devono avere una copertina con un'etichetta di classificazioneevidente e un'altra su ogni pagina, visibile quando viene aperto il documento. Tutti i file elettronici non etichettabili facilmente (database o file grezzi) devono essere protetti da controlli all'accesso, per garantire che queste informazioni non siano diffuse in modo scorretto e non siano manipolate, distrutte o rese inaccessibili. Tutti i supporti informatici quali dischetti, nastri e CD-ROM devono essere etichettati in base al livello più alto di classificazione delle informazioni contenute.

Diffusione delle informazioni

La diffusione delle informazioni significa la rivelazione dei dati alle varie parti in base alla loro identità e autorizzazione all'accesso.

Procedura di verifica del dipendente

Politica: l'azienda dovrebbe prevedere procedure esaustive utilizzabili dai dipendenti per verificare l'identità, l'incarico e l'autorizzazione dell'individuo prima di diffondere informazioni confidenziali o sensibili o di eseguire una procedura che implica l'uso di hardware o software informatico.

Spiegazione/Note: laddove giustificato dalle dimensioni dell'azienda e dai bisogni specifici di protezione, andrebbero utilizzate le tecnologie avanzate di sicurezza per verificare l'identità. La misura migliore sarebbe usare apparecchi di verifica insieme a un segreto condiviso per identificare positivamente le persone che avanzano la richiesta. Per

quanto questa pratica possa ridurre il rischio in maniera significativa, il costo potrebbe essere proibitivo per certe imprese. In questi casi. l'azienda dovrebbe utilizzare solo un segreto condiviso, come una password o un codice giornaliero.

Diffusione di informazioni a terzi

Politica: prevedete un insieme di procedure raccomandate per la diffusione di informazioni, che tutti i dipendenti devono essere preparati a seguire.

Spiegazione/Note: in genere bisogna imporre queste procedure di distribuzione per:

- Informazioni libere all'interno dell'azienda.
- Distribuzione di informazioni a individui e dipendenti di organizzazioni che hanno un rapporto consolidato con l'azienda, quali consulenti, lavoratori a tempo determinato, interni, personale di strutture fornitrici o consociate ecc.
- Informazioni disponibili per l'esterno.
- Informazioni a qualsiasi livello di classificazione qualora siano diffuse di persona, per telefono, per posta anche elettronica, per fax, per casella vocale, per corriere e mezzo elettronico.

Diffusione di informazioni confidenziali

Politica: le informazioni confidenziali, cioè quelle che potrebbero provocare danni notevoli qualora ottenute da persone non autorizzate, possono essere rilasciate soltanto a persona fidata autorizzata.

Spiegazione/Note: le informazioni confidenziali in forma fisica (cioè stampate o su supporto rimovibile) possono essere diffuse:

- Di persona.
- Tramite posta interna sigillata e contrassegnata come "confidenziale".
- Fuori dall'azienda tramite un corriere fidato (per esempio Federal Express, UPS e simili) con firma obbligatoria del ricevente, o da un servizio postale che prevede una classe di posta raccomandata.

Le informazioni confidenziali sotto forma elettronica (file, database, e-mail) possono essere diffuse:

- All'interno di una e-mai1 cifrata.
- Come allegato sotto forma di file cifrato.
- Tramite trasferimento elettronico a un server della rete interna dell'azienda.
- Da un programma fax del computer, ammesso che soltanto il destinatario previsto usi la macchina all'altro capo o che lo stia aspettando presso quella macchina. Come alternativa, potete mandare fax senza la presenza del destinatario se usate un collegamento telefonico crittato a un server fax protetto da password.

Le informazioni confidenziali possono essere discusse di persona, per telefono all'interno dell'azienda, per telefono esterno se esiste la cifratura, per trasmissione satellitare crittata, per collegamento crittato in videoconferenza e per Voice Over Internet Protocol (VOIP) crittato.

Per le tramissioni via fax, il metodo raccomandato prevede che il mittente trasmetta una copertina e che il destinatario mandi una pagina di risposta appena la riceve per dimostrare che è alla macchina, dopodiché il mittente invierà il fax.

Non sono accettabili per discutere o diffondere informazioni confidenziali i seguenti mezzi di comunicazione: e-mail in chiaro, messaggi di casella vocale, posta normale e metodi di comunicazione senza fili, wireless (cellulari, cordless, sms).

Diffusione di informazioni personali

Politica: le informazioni personali, cioè quelle sui dipendenti che, se portate a conoscenza, potrebbero danneggiare loro o l azienda, possono essere diffuse solo a persona fidata autorizzata.

Spiegazione/Note: le informazioni personali in forma fisica (cioè su carta o su supporto d'archivio) possono essere diffuse:

- Di persona.
- Tramite posta interna sigillata e contrassegnata come "personale".
- Tramite posta normale.

Le informazioni personali in forma elettronica (file, database, e-mail) possono essere diffuse:

- Tramite posta elettronica interna.
- Tramite trasferimento elettronico a un server della rete interna dell'azienda.
- Per facsimile, ammesso che soltanto il destinatario previsto usi la macchina all'altro capo o che stia aspettando il fax presso quella macchina. Potete spedirli anche a server fax protetti da password. Come alternativa, potete mandare fax senza la presenza del destinatario se inviati tramite collegamento telefonico crittato a un server fax protetto da password.

Le informazioni personali possono essere discusse di persona, per telefono, per satellite, per videoconferenza e VOIP crittato.

Non sono accettabili per discutere o diffondere informazioni personali i seguenti mezzi di comunicazione: e-mail in chiaro, messaggi di voice mail, posta normale e metodi di comunicazione senza fili (cellulari, cordless, sms).

Diffusione delle informazioni interne

Politica: le informazioni a uso interno sono quelle da condividere solo internamente all'azienda o con persone fidate che hanno firmato un accordo di riservatezza. Bisogna prevedere delle linee guida per la diffusione delle informazioni interne.

Spiegazione/Note: le informazioni interne possono essere distribuite in ogni forma, compresa la posta elettronica aziendale, ma non fuori dall'azienda a meno che le e-mail non siano cifrate.

Discutere informazioni delicate per telefono

Politica: prima di dare per telefono informazioni che non sono state dichiarate pubbliche, la persona che le fornisce deve riconoscere la vo-

ce del richiedente per previi contatti di lavoro, oppure se il sistema telefonico ha identificato la chiamata come proveniente dall'interno assegnato al richiedente.

Spiegazione/Note: se la voce del richiedente non è nota, chiamate il suo interno per controllarla sul messaggio registrato in segreteria oppure il suo superiore per controllare l'identità e l'autorizzazione all'accesso.

Procedure del personale all'ingresso o *all'accoglienza*

Politica: il personale nell'atrio deve farsi consegnare un documento con foto prima di affidare un plico a qualsiasi persona che non sia nota come dipendente in ruolo. Occorrerebbe un registro su cui segnare nome, numero del documento d'identità, data di nascita, oggetto prelevato e ora e data del prelievo.

Spiegazione/Note: questa politica si applica anche per la consegna dei pacchetti in uscita a qualsiasi fattorino o corriere. Le compagnie come Federa1 Express usano tesserini di riconoscimento per i loro dipendenti.

Trasferimento di *software* a terzi

Politica: prima di consegnare o rivelare programmi o istruzioni dei computer, dovete verificare l'identità del richiedente e capire se questa consegna è coerente con la classificazione assegnata a queste informazioni. Di norma, i programmi sviluppati in sede in formato source-code sono considerati rigorosamente proprietà riservata e classificati come confidenziali.

Spiegazione/Note: la decisione dell'autorizzazione si basa di solito sulla necessità del richiedente di accedere al software per il proprio lavoro.

Abilitare la posizione del cliente

Politica: il personale addetto a vendite e marketing deve verificare la posizione prima di dare numeri di telefono, piani di produzione, contatti nel gruppo di produzione o altre informazioni delicate a qualsiasi cliente potenziale.

Spiegazione/Note: è una tattica usuale dello spionaggio industriale entrare in contatto con un responsabile marketing e vendite per fargli credere che è in vista un grosso ordine. Per approfittare di questa occasione il responsabile spesso rivela informazioni utilizzabili successivamente dall'attaccante come moneta di scambio per avere accesso a informazioni delicate.

Trasferimento di file o dati

Politica: i file e gli altri dati elettronici non dovrebbero essere trasferiti su altri supporti rimovibili a meno che il richiedente sia persona fidata identificata e con diritto di disporre di quei dati in quel formato.

Spiegazione/Note: un ingegnere sociale può facilmente ingannare un dipendente fornendo una richiesta plausibile per farsi copiare le informazioni sensibili su nastro, Zip o altro supporto rimovibile e farsele inviare oppure conservare all'ingresso per un successivo prelievo.

Gestione telefoni

Le politiche di gestione dei telefoni garantiscono che i dipendenti possano verificare l'identità di chi chiama e proteggere da chi chiama le proprie informazioni come contatto.

Trasferimento di chiamata su numeri di modern o di fax

Politica: i servizi di trasferimento di chiamata che permettono di passare le telefonate a numeri esterni non saranno attivati su modem o numeri di fax all'interno dell'azienda.

Spiegazione/Note: gli attaccanti sofisticati possono tentare di ingannare il personale dell azienda del telefono o i lavoratori delle telecomunicazioni interne affinché attivino il trasferimento di chiamata da un
: a una linea e: controllata dall'attaccante. Ques tattica
tt all'intruso di intercettare fax, richiedere l'invio per f di
informazioni riservate all'interno dell'azienda (il personale dà per scontato che un fax all'interno della struttura sia sicuro), oppure convincere chi si è collegato a fornire la sua vassword facendo slittare la chiamata a un computer trappola che simula la procedura di log-in.

A seconda dei servizi telefonici dell'azienda, il trasferimento di chiamata può essere controllato dal provider e non dal settore telecomunicazioni. In questo caso, sarà fatta una richiesta al provider affinché l'opzione trasferimento di chiamata non sia presente sui numeri assegnati alle linee di fax e modem.

Identificazione di chiamata

Politica: il sistema telefonico aziendale deve fornire l'identificazione di chiamata su tutti gli ayyarecchi interni e, yossibilmente. uno sauillo diverso quando la telefonata proviene da fuori.

Spiegazione/Note: se i dipendenti possono verificare l'identità di chi telefona da fuori possono sventare un attacco o identificare l'attaccante presso il personale addetto alla sicurezza.

Telefoni di cortesia

Politica: per impedire che i visitatori si facciano passare per dipendenti, ogni telefono di cortesia indicherà con chiarezza la localizzazione di chi chiama (per esempio "atrio") sull'identificatore di chiamata del ricevente.

Spiegazione/Note: se l'identificazione di chiamata per le telefonate interne mostra solo il numero d'interno, bisogna pensare alla possibilità di una chiamata proveniente dai telefoni in sala d'aspetto o in altre aree pubbliche. Non dev'essere possibile che l'attaccante faccia una chiamata da uno di questi apparecchi per indurre un dipendente a credere che arrivi da un collega.

Password in default del fabbricante allegate ai sistemi telefonici

Politica: l'amministratore delle caselle vocali dovrebbe cambiare tutte le password di default allegate alla rete telefonica prima dell'utilizzo da parte del personale.

Spiegazione/Note: gli ingegneri sociali possono ottenere gli elenchi delle password di default dai fabbricanti e usarle per accedere agli account amministratore.

Caselle vocali di settore

Politica: installate una casella vocale generica per ogni ufficio che è in regolare contatto con il pubblico.

Spiegazione/Note: il primo passo dell'ingegnere sociale è la raccolta di informazioni sull'azienda bersaglio e sul suo personale. Limitando l'accesso a nomi e numeri di telefono di dipendenti, un'azienda gli renderà più difficile identificare i bersagli dentro la compagnia oppure usare i nomi dei legittimi dipendenti per ingannare altri colleghi.

Verifica dell'assistenza al sistema telefonico

Politica: nessun tecnico dell'assistenza potrà accedere dall'esterno al sistema telefonico aziendale senza un'identificazione positiva e un'autorizzazione a eseguire il suo lavoro.

Spiegazione/Note: gli intrusi informatici, accedendo ai sistemi telefonici aziendali, possono creare caselle vocali, intercettare i messaggi diretti ad altri oppure fare telefonate gratis a spese vostre.

Configurazione del sistema telefonico

Politica: l'amministratore delle caselle vocali rispetterà le esigenze di sicurezza generale configurando gli adatti parametri di sicurezza nel sistema telefonico.

Spiegazione/Note: i sistemi telefonici possono essere installati con vari gradi di sicurezza per i messaggi vocali. L'amministratore dovrebbe essere consapevole delle esigenze di tutela della compagnia e lavorare con il personale addetto alla sicurezza in modo da configurare il sistema telefonico affinché protegga i dati delicati.

Opzione rintracciamento della chiamata

Politica: a seconda delle limitazioni del provider di telecomunicazioni, l'opzione per rintracciare la chiamata sarà attivata globalmente per permettere agli impiegati di usarla nel caso in cui sospettino che sia un attaccante a chiamare.

Spiegazione/Note: i dipendenti devono essere addestrati a usare l'opzione e informati sulle circostanze giuste per usarla. Il rintracciamento della chiamata dovrebbe essere avviato quando chi telefona sta chiaramente tentando di accedere non autorizzato ai sistemi informatici aziendali o sta richiedendo informazioni riservate. Ogni volta che un dipendente attiva l'opzione occorre inviare notifica al gruppo preposto alla segnalazione degli incidenti.

Sistemi telefonici automatizzati

Politica: se l'organizzazione usa un sistema di risposta automatizzata, esso deve essere programmato in modo che gli interni non siano annunciati quando si passa una chiamata a un dipendente o a un ufficio.

Spiegazione/Note: gli attaccanti possono usare il sistema telefonico automatizzato per farsi un'idea dei nomi e degli interni del personale. A quel punto sfrutteranno gli interni per far credere a chi risponde di essere dei colleghi aventi diritto alle informazioni riservate al personale.

Caselle vocali disattivate dopo una serie di tentativi falliti di accesso

Politica: programmate il sistema telefonico aziendale in modo da escludere qualsiasi account vocale ogni volta che viene fatto un dato numero di tentativi falliti di accesso.

Spiegazione/Note: l'amministratore delle telecomunicazioni deve escludere una casella vocale dopo cinque successivi tentativi falliti di log-in, poi resettare manualmente ogni blocco di casella vocale.

Interni telefonici limitati

Politica: Tutti gli interni di uffici o di settori che solitamente non ricevono chiamate dall'esterno (ufficio assistenza, sala informatica, assistenza tecnica dipendenti ecc.) dovrebbero essere programmati in modo che questi telefoni siano raggiungibili solo dall'interno. Altrimenti vanno protetti con una password in modo che il personale e le persone autorizzate, che chiamano da fuori, debbano inserire la parola d'ordine corretta.

Spiegazione/Note: anche se questa contromisura frustrerà quasi tutti i tentativi degli ingegneri sociali dilettanti per arrivare ai probabili bersagli, dovrebbe essere ricordato che un attaccante deciso riuscirà talvolta a convincere un dipendente a chiamare l'interno ad accesso limitato chiedendo alla persona che risponderà di telefonare all'attaccante, oppure di passargli l'interno in questione. Durante il training alla sicurezza, occorre discutere bene questo metodo di convincere i dipendenti a dare una mano all'intruso, per renderli edotti di queste tattiche.

Miscellanea

Struttura del tesserino d'identificazione

Politica: i tesserini di riconoscimento devono essere fatti in modo da comprendere una grande foto riconoscibile da lontano.

Spiegazione/Note: la fotografia classica sui tesserini è meglio di niente per quanto riguarda la sicurezza. La distanza tra una persona che entra nel palazzo e il custode o addetto all'accoglienza, che deve controllare l'identità, è di solito abbastanza grande perché la foto si dimostri troppo piccola per riconoscere la persona mentre passa. Perché sia utile, è necessario riprogettare il tesserino, se necessario.

Revisione dei diritti di accesso quando si cambia posizione o responsabilità

Politica: ogni volta che un dipendente cambia ruolo o gli vengono affidate responsabilità maggiori o minori, il suo superiore awertirà la IT di questa novità perché possa essergli assegnato un adeguato profilo di sicurezza.

Spiegazione/Note: la gestione dei diritti di accesso del personale è necessaria per limitare la rivelazione di informazioni protette. Si applicherà la regola del *minor privilegio:* i diritti di accesso assegnati agli utenti saranno i minimi necessari per eseguire quel lavoro. Ogni richiesta di cambiamento che risulti in diritti accresciuti deve concordare con una politica di concessione di accrescimento diritti.

Il superiore del lavoratore oppure il settore risorse umane avrà la re-

sponsabilità di notificare il settore Information Technology perché adegui i diritti di accesso del detentore di account.

Identificazione speciale per gli esterni

Politica: La vostra azienda dovrebbe rilasciare un pass speciale con foto per gli addetti alle consegne fidati e per i non dipendenti che devono entrare nei vostri locali regolarmente.

Spiegazione/Note: Gli esterni che devono entrare nell'edificio regolarmente (per esempio per le consegne di vivande alla mensa oppure per riparare la macchina delle fotocopie o installare telefoni) possono costituire una minaccia. Oltre a rilasciare materiali di identificazione per questi visitatori, verificate che i vostri dipendenti siano allenati a individuare un visitatore privo di pass e sappiano come comportarsi in questa situazione.

Disabilitare gli account per i fornitori

Politica: ogni volta che un fornitore cui è stato assegnato un account informatico ha concluso il suo rapporto. o quando scade il contratto, il caposettore responsabile notificherà immediatamente al settore Information Technology affinché disabiliti gli account, compresi quelli usati per accedere al database, al modem o per l'accesso Internet in remoto.

Spiegazione/Note: terminato un rapporto di lavoro c'è sempre il pericolo che gli altri usino la conoscenza dei sistemi e delle procedure della vostra azienda per accedere ai dati. Tutti gli account informatici usati da quella persona o a lui noti devono essere subito disabilitati. Ciò comprende anche gli account dei database della produzione, quelli di collegamento remoto e tutti quelli usati per accedere ad apparecchi informatici.

Organizzazione del sistema di segnalazione incidenti

Politica: dovrete allestire una struttura per segnalare gli incidenti oppure, nelle aziende più piccole, un singolo individuo e una riserva per ricevere e diffondere gli allarmi riguardo presunti incidenti in corso relativi alla sicurezza.

Spiegazione/Note: centralizzando le segnalazioni di presunti incidenti, un attacco che altrimenti sarebbe passato inosservato può essere scoperto. Nel caso siano scoperti e segnalati sistematici attacchi all'organizzazione, la struttura di segnalazione dev'essere in grado di intuire che cosa sta prendendo di mira l'attaccante in modo da poter decidere contromisure speciali per proteggere quei beni.

I dipendenti delegati a ricevere le segnalazioni devono conoscere alla perfezione i metodi e le tattiche degli ingegneri sociali, in modo da poter valutare le segnalazioni e capire quando è in corso un attacco.

Hot line per segnalare gli incidenti

Politica: prevedete una hot line collegata alla struttura di segnalazione incidenti o con la persona delegata, che potrebbe essere un interno facile da ricordare.

Spiegazione/Note: quando un membro del personale sospetta di essere bersaglio di un attacco, dev'essere in grado di notificare immediatamente alla struttura di segnalazione. Perché questa notizia sia tempe-

stiva, tutti gli operatori e centralinisti dell'azienda devono avere il numero in bella vista.

Un sistema di allerta tempestiva a livello aziendale può aiutare in maniera significativa l'organizzazione nel rilevamento e nella risposta a un attacco in corso. I dipendenti devono essere adeguatamente preparati in modo che appena sospettano di essere vittima di un attacco chiamino immediatamente la hot line. Secondo le procedure stabilite, il personale addetto alla segnalazione incidenti avvertirà immediatamente i gruppi bersaglio dell'intrusione possibile in modo da tenere alta la soglia d'attenzione. Perché la segnalazione sia tempestiva. il numero della hot line dev'essere conosciuto in tutta la struttura.

Sigillare le aree delicate

Politica: una guardia filtrerà l'accesso alle aree sicure o delicate, chiedendo due forme di autentica.

Spiegazione/Note: una forma accettabile di autentica è una serratura elettronica in cui il dipendente deve passare il tesserino e inserire un codice d'accesso. Il miglior metodo per recintare le aree delicate è una guardia a ogni entrata. Nelle organizzazioni in cui sarebbe troppo costoso, usate due forme di convalida dell'identità. A seconda dei rischi e del costo, si raccomanda una carta d'accesso biometrica.

Ripostigli per le reti e per le telecomunicazioni

Politica: i ripostigli e le stanze contenenti i cavi di rete o del telefono o i punti di accesso alla rete devono essere sempre sorvegliati.

Spiegazione/Note: soltanto il personale autorizzato potrà accedere ai ripostigli o agli stanzini delle telecomunicazioni. I manutentori esterni o i fornitori devono essere identificati con certezza. usando le procedure diffuse dall'ufficio preposto alla sicurezza delle informazioni. L'accesso alle linee telefoniche, agli hub di rete, ai centralini e agli altri macchinari correlati potrebbe essere usato dagli attaccanti per compromettere la sicurezza dei computer o della rete.

Cassette della posta interna

Politica: le cassette per la posta interna non devono essere piazzate in aree accessibili a tutti.

Spiegazione/Note: le spie industriali o gli intrusi informatici capaci di accedere ai punti di raccolta della posta interna possono inviare facilmente autorizzazioni false o moduli che permettono al personale di diffondere informazioni confidenziali o a fare qualcosa che aiuti il malintenzionato. Inoltre, l'attaccante può mandare un floppy o un altro supporto elettronico con istruzioni di installare un aggiornamento di programma oppure di aprire un file con all'interno comandi macro che servono ai fini dell'intruso. Naturalmente ogni richiesta arrivata per posta interna viene data per scontata come autentica da chi la riceve.

Bacheca aziendale

Politica: le bacheche per i lavoratori non devono essere piazzate in punti in cui ha accesso il pubblico.

Spiegazione/Note: molte imprese hanno delle bacheche in cui si affiggono informazioni riservate o personali affinché tutti le leggano. Spesso vi si attaccano annunci dei datori di lavoro, liste dipendenti, promemoria

interni, numeri di contatto privati dei dipendenti elencati nelle pubblicità e altre informazioni consimili.

Le bacheche possono essere piazzate presso la mensa o vicino alle aree fumatori o di riposo cui i visitatori hanno accesso illimitato. Questo genere di informazioni non dovrebbe essere messo a disposizione di visitatori o pubblico.

Entrata del centro informatico

Politica: la sala computer o il centro dati devono essere sempre sbarrati e il personale deve autenticare la propria identità prima di entrare.

Spiegazione/Note: la sicurezza aziendale dovrebbe pensare se sia il caso di distribuire un tesserino elettronico o un lettore di card perché tutti gli accessi siano controllati e memorizzati elettronicamente.

Account clienti presso i provider di un servizio

Politica: il personale che passa gli ordini ai fornitori di servizi critici per l'azienda deve prevedere una password degli account per impedire a persone non autorizzate di fare ordini per conto dell'azienda.

Spiegazione/Note: i fornitori di servizi permettono ai clienti su richiesta di decidere una password. L'azienda dovrebbe stabilire password per tutti i fornitori di servizi critici. Questa politica è fondamentale soprattutto per quanto riguarda telecomunicazionee Internet. Ogni volta che un servizio essenziale è compromesso, è necessario verificare un segreto condiviso prima che chi chiama sia autorizzato a fare un ordine. Ricordate anche che gli identificatori classici quali il numero della previdenza sociale o di matricola aziendale, il cognome da ragazza della madre o simili non devono essere usati. Per esempio, un ingegnere sociale potrebbe chiamare la compagnia dei telefoni per ordinare di aggiungere opzioni come il trasferimento di chiamata su linee dial-in oppure richiedere al provider di Internet di cambiare le informazioni di traduzione in modo da fornire un indirizzo IP fasullo quando gli utenti eseguono una ricerca hostname.

Contatto di dipartimento

Politica: la vostra compagnia potrebbe avviare un programma in cui ogni settore o ufficio affida a un dipendente la responsabilità di fungere da punto di contatto perché ogni lavoratore possa verificare con facilità l'identità degli sconosciuti che sostengono di venire da quel settore. Per esempio, l'ufficio assistenza può chiamare questa persona di contatto per verificare l'identità di un dipendente che richiede un intervento.

Spiegazione/Note: questo metodo di verifica dell'identità riduce il novero dei dipendenti autorizzati a garantire per i colleghi nel proprio settore quando richiedono assistenza come in caso di resettaggio delle password o per altri problemi informatici. Gli attacchi degli ingegneri sociali hanno successo anche perché il personale dell'assistenza tecnica è sempre pressato e non verifica in modo adeguato l'identità dei richiedenti. Di solito, nelle grandi organizzazioni non è possibile conoscere di persona tutti gli autorizzati per via dell'elevato numero di lavoratori. Il metodo del contatto singolo per le garanzie limita il numero di dipendenti che l'assistenza tecnica deve conoscere personalmente a fini di verifica.

Password clienti

Politica: i rappresentanti dei servizi per la clientela non potranno recuperare le password degli account clienti.

Spiegazione/Note: spesso gli ingegneri sociali chiamano il servizio clienti e tentano con un pretesto di strappare un'informazione sull'autentica del cliente come una password o il numero della previdenza sociale. Poi, forti di questa informazione, chiamano un altro servizio fingendo di essere il cliente e ottengono dati oppure fanno ordini fraudolenti. Per impedire il successo di questi tentativi occorre allestire un software per il servizio clienti in modo che i rappresentanti possano solo digitare le informazioni di autentica fornite dal chiamante ricevendo una risposta dal sistema a conferma della correttezza o meno della password.

Test di vulnerabilità

Politica: è consigliabile la notifica durante il training e l'orientamento del dipendente dell'utilizzo periodico da parte dell'azienda delle tattiche degli ingegneri sociali per saggiare i punti deboli della sicurezza.

SpiegazionNote: senza questa notifica dei test di penetrazione, il personale potrebbe essere imbarazzato, arrabbiarsi o subire altri traumi psichici a causa dell'uso di tecniche ingannevoli contro di loro da parte di colleghi o incaricati. Se si awertono durante il periodo di orientamento i nuovi assunti che possono essere sottoposti a esami del genere, preverrete questi attriti.

Esposizione delle informazioni confidenziali

Politica: le informazioni aziendali non previste per la diffusione pubblica non saranno esposte in aree accessibili a tutti.

SpiegazionNote: oltre alle informazioni confidenziali sui prodotti o la procedura, saranno parimenti tenute sotto chiave le informazioni a uso interno come gli elenchi dipendenti o i numeri di telefono o gli organigrammi di ogni settore.

Training di attenzione alla sicurezza

Politica: tutte le persone impiegate dall'azienda devono completare durante la fase di orientamento, un periodo di addestramento che le informi sui problemi della sicurezza. Inoltre, ogni dipendente deve seguire corsi di aggiornamento a intervalli periodici, non oltre i dodici mesi, come richiesto dal dipartimento incaricato del training.

Spiegazione/Note: molte organizzazioni snobbano del tutto il training. Stando all'analisi Global Information Security Survey del 2001, soltanto il trenta percento delle organizzazioni prese in esame investono nel training, che invece è essenziale per minimizzare le falle nella sicurezza tramite tecniche di ingegneria sociale.

Corsi di preparazione alla sicurezza prima di ottenere l'accesso ai computer

Politica: il personale deve frequentare e completare con successo un corso di informazione sui temi della sicurezza prima che gli sia consentito accedere ai sistemi informatici aziendali.

Spiegazione/Note: spesso gli ingegneri sociali prendono di mira i

nuovi assunti sapendo che sono in genere quelli meno al corrente delle politiche di sicurezza e delle procedure per decidere la classificazione e la gestione delle informazioni delicate.

Il training dovrebbe prevedere un'occasione in cui i dipendenti possano porre domande su queste politiche. Dopo l'addestramento, il titolare dell'account dovrai firmare di aver compreso le politiche di sicurezza dando conferma che le osserverà.

Tesserino a codice colore

Politica: i tesserini di identificazione devono utilizzare un codice colore per indicare se il possessore è un dipendente, un incaricato esterno, un lavoratore a tempo determinato, un fornitore, un consulente, un visitatore o uno stagista.

Spiegazione/Note: il colore del tesserino è un mezzo eccellente per cogliere al volo da lontano lo status di una persona. L'alternativa potrebbe essere l'uso di caratteri più grandi nella scritta del ruolo, però il codice colore è inconfondibile e facile da individuare. Un classico trucco degli ingegneri sociali per accedere ai palazzi è quello di travestirsi da fattorino o riparatore. Una volta all'interno della struttura si camufferanno da dipendente oppure mentiranno per ottenere la collaborazione dei colleghi ignari. Perciò questa politica impedirà loro di entrare in modo legittimo nella struttura per poi infiltrarsi in aree in cui non devono avere accesso. Per esempio, una persona entrata come tecnico dei telefoni non può farsi passare per un dipendente: il colore del tesserino lo smaschererà subito.

POLITICHE SULLA INFORMATION TECHNOLOGY

Il settore Information Technology di ogni azienda necessita di politiche speciali che aiutino a proteggere le informazioni della compagnia. Per rispecchiare la tipica struttura dell'ufficio IT di un'organizzazione, ho suddiviso le politiche relative in generiche, assistenza, amministrazione computer e centrale operativa.

Generiche

Informazioni sui dipendenti del settore IT

Politica: i numeri di telefono e gli indirizzi e-mail dei singoli dipendenti del settore non saranno rivelati a nessuno che non sia autorizzato.

Spiegazione/Note: lo scopo di questa politica è di prevenire l'abuso delle informazioni da parte degli ingegneri sociali. Rivelando solo il numero generico o l'indirizzo di e-mail del settore IT impedirete agli esterni di entrare direttamente in contatto con il personale del settore. L'indirizzo di e-mail dei contatti tecnici e della gestione del sito dovrebbe essere soltanto un nome generico come admin@nomeazienda.com.I numeri telefonici pubblici dovrebbero essere collegati con una casella vocale di dipartimento, non con i singoli lavoratori.

Quando le informazioni per i contatti diretti sono disponibili, allora è semplice per l'intruso informatico raggiungere specifici dipendenti

dell'IT convincendoli a fornire informazioni utilizzabili in un attacco oppure impersonando colleghi usando il loro nome o le informazioni per il contatto.

Richieste di assistenza tecnica

Politica: tutte le richieste di assistenza tecnica devono essere rivolte al gruppo che le gestisce.

Spiegazione/Note: gli ingegneri sociali potrebbero tentare di prendere di mira il personale IT che, di regola, non gestisce i problemi tecnici e che potrebbe non conoscere le corrette misure di sicurezza quando risponde a tali richieste. Inoltre il personale IT dev'essere preparato a non obbedire a queste richieste e rimandare l'interlocutore al gruppo incaricato dell'assistenza.

Ufficio help desk

Procedure di accesso remoto

Politica: il personale dell'assistenza non deve divulgare dettagli o istruzioni sull'accesso remoto, compresi i punti esterni di accesso alla rete o i numeri dei modem, a meno che il richiedente non sia stato:

- Verificato come persona autorizzata a ricevere informazioni interne.
- Verificato come persona autorizzata a collegarsi alla rete aziendale come utente esterno. Se non è noto di persona, il richiedente dovrà essere identificato in conformità con le procedure di verifica e autorizzazione esposte all'inizio di questo capitolo.

Spiegazione/Note: il servizio assistenza interna è spesso il primo bersaglio dell'ingegnere sociale sia per la natura del suo lavoro, c i ~ & are una mano in caso di problemi informatici, sia perché di solito ha privilegi elevati di sistema. Tutto il personale di questo ufficio dev'essere preparato a comportarsi da firewall umano per impedire diffusioni non autorizzate di informazioni, che potrebbero aiutare persone non autorizzate ad accedere alle risorse aziendali. La regola fondamentale è non rivelare mai le procedure di accesso remoto a nessuno prima di un'identificazione.

Cambiare le password

Politica: la password di un account può essere cambiata solo su richiesta del titolare dell'account.

Spiegazione/Note: il trucco più comune usato dagli ingegneri sociali è il cambio della password di un'altra persona. L'attaccante finge di essere un dipendente e di avere perso o dimenticato la password. Per ridurre le possibilità di successo di questo genere di attacco, un dipendente del settore IT che riceve una richiesta di cambiamento password deve richiamare il lavoratore prima di muovere un dito, e la telefonata non dev'essere fatta al numero fornito dal richiedente bensì a quello che figura in elenco. Vedi le procedure di verifica e autorizzazione riguardo questa misura.

Cambiare i privilegi di accesso

Politica: tutte le richieste di aumentare i privilegi o i diritti di accesso devono essere approvate per iscritto dal superiore del titolare dell'account. Una volta apportato il cambiamento sarà necessario mandare una conferma al capoufficio richiedente tramite posta interna. Inoltre queste richieste devono essere verificate secondo le procedure di verifica e autorizzazione.

Spiegazione/Note: una volta che un intruso informatico ha compromesso un normale account, il passo successivo sarà di elevare i relativi privilegi in modo da avere il completo controllo del sistema infiltrato. Un attaccante a conoscenza dei processi di autorizzazione può fingere una richiesta autorizzata quando è trasmessa per e-mail, fax o telefono. Per esempio, può telefonare all'assistenza generica o a quella informatica per convincere un tecnico a garantire ulteriori diritti di accesso all'account compromesso.

Autorizzazione di un nuovo account

Politica: una richiesta di nuovo account per un dipendente, incaricato o altra persona autorizzata dev'essere fatta o per iscritto firmata dal superiore oppure tramite e-mail con firma digitale. Queste richieste devono essere verificate anche mandando una conferma tramite posta interna.

Spiegazione/Note: visto che le password e le altre informazioni utili per entrare nei sistemi informatici sono i primissimi bersagli dei ladri di informazioni per guadagnarsi l'accesso, si rendono necessarie precauzioni speciali. L'intento di questa politica è di impedire agli intrusi informatici di fingersi personale autorizzato o di falsificare le richieste di nuovo account. Perciò tutte queste richieste devono essere confermate secondo le procedure di verifica e autorizzazione.

Consegna delle nuove password

Politica: le nuove password devono essere gestite come informazioni confidenziali, e consegnate con metodi sicuri come per esempio di persona, in una spedizione con ricevuta di ritorno o tramite corriere fidato. Vedi le politiche sulla distribuzione delle informazioni confidenziali.

Spiegazione/Note: potete usare anche la posta interna ma si raccomanda che le password siano contenute in buste sigillate così da oscurare il contenuto. Un metodo consigliato è di designare un contatto informatico in ogni settore con la responsabilità di gestire la distribuzione dei dettagli sui nuovi account e garantire l'identità del personale che perde o dimentica la password. In questi casi il personale di appoggio lavorerà sempre con un gruppo ridotto di colleghi rispetto a quelli che conosce di persona.

Disattivare un account

Politica: prima di disattivare un account dovete chiedere conferma che la richiesta sia stata fatta da una persona autorizzata.

Spiegazione/Note: questa politica vuole impedire che qualcuno falsifichi una richiesta di disabilitare un account e poi chiami per risolvere l'impossibilità dell'utente ad accedere al sistema. Quando l'ingegnere sociale telefona fingendosi un tecnico a conoscenza dell'impossibilità

della vittima a connettersi, questi spesso obbedisce a una richiesta di rivelare la sua password durante la sistemazione del problema.

Disabilitare porte seriali di rete o altri macchinari

Politica: nessun dipendente disabiliterà alcun apparecchio di rete o porta seriale per conto di tecnici non verificati.

Spiegazione/Note: questa politica serve a prevenire una falsa richiesta di disabilitazione di una porta di rete, per poi chiamare l'utente dicendo che gli si risolverà il problema di accesso alla rete. Quando l'ingegnere sociale, fingendosi tecnico comprensivo, telefona dimostrando di conoscere il problema della vittima, durante la sistemazione del problema il bersaglio obbedisce facilmente a un'eventuale richiesta di rivelare la propria password.

Rivelazione di procedure per accesso wireless

Politica: nessun membro del personale dovrebbe rivelare ai non autorizzati alla connessione le procedure per accedere ai sistemi aziendali su reti wireless.

Spiegazione/Note: esigete sempre una pregressa verifica del richiedente come persona autorizzata a connettersi alla rete aziendale in veste di utente esterno prima di spiegare l'accesso wireless. Vedi "Procedure di verifica e autorizzazione".

Notifica problemi

Politica: i nomi dei dipendenti che hanno segnalato problemi legati al computer non dovrebbero essere diffusi fuori dal settore Information Technology.

Spiegazione/Note: in un tipico attacco, l'ingegnere sociale chiamerà il servizio assistenza chiedendo il nome di un dipendente che ha segnalato recentemente problemi al computer. Potrebbe fingere di essere un collega, un fornitore o un tecnico dell'azienda telefonica, e una volta ottenuti i nomi di chi ha segnalato qualche guaio li contatterà dicendo che sta chiamando per risolverli. Durante la telefonata ingannerà la vittima per ottenere l'informazione desiderata o far eseguire un'azione che lo aiuti.

Esecuzione comandi o apertura programmi

Politica: il personale del settore IT in possesso di account privilegiati non dovrebbe eseguire comandi o aprire applicazioni su richiesta di una persona che non gli è nota.

Spiegazione/Note: un classico metodo usato dagli attaccanti per installare un cavallo di Troia o altri software pericolosi consiste nel cambiare il nome di un programma già esistente, poi chiamare l'assistenza informatica lamentando un messaggio di errore che compare ogni volta che tenta di aprirlo e convincendo il tecnico a farlo per conto suo. Quando questi esegue, il *malware* eredita i privilegi dell'utente che esegue il programma e compie una task, dando così all'attaccante gli stessi privilegi informatici del tecnico dell'assistenza. In questo modo l'attaccante può assumere il controllo del sistema aziendale. Questa politica introduce una contromisura a una manovra del genere, richiedendo al personale di appoggio di verificare la carica del collega prima di aprire un programma su richiesta di uno che telefona.

Cambiare i diritti globali di accesso

Politica: una richiesta di cambiare i diritti globali di accesso correlati a un profilo di lavoro nel settore elettronico dovrebbe essere approvata dal gruppo cui è delegata la responsabilità di gestire i diritti di accesso sulla rete aziendale.

Spiegazione/Note: il personale autorizzato analizzerà ogni richiesta del genere per decidere se il cambiamento potrebbe comportare una minaccia alla sicurezza delle informazioni. In questo caso il responsabile appianerà con il richiedente i vari problemi per arrivare insieme a una decisione sui cambiamenti da apportare.

Richieste di accesso remoto

Politica: l'accesso remoto informatico sarà fornito solo al personale che avrà dimostrato una reale necessità di accedere ai sistemi informatici aziendali dall'esterno. La richiesta dev'essere presentata da un caposettore e verificata come descritto nella sezione "Procedure di verifica e autorizzazione".

Spiegazione/Note: una valutazione della necessità di accesso dall'esterno alla rete aziendale da parte del personale autorizzato, limitandolo solo alle persone che ne hanno assoluta necessità, potrebbe ridurre in maniera esponenziale i rischi e i problemi gestionali degli utenti in accesso remoto. Meno sono le persone con privilegi di connessione via modem, più ristretto è il novero dei potenziali bersagli di un attacco. Non dimenticate mai che l'attaccante può prendere di mira gli utenti remoti per dirottare la loro connessione alla rete aziendale oppure facendosi passare per loro in una telefonata pretesto.

Cambiare le password di account privilegiato

Politica: un'eventuale richiesta di sistemare una password di un account privilegiato dev'essere approvata dal manager o amministratore di sistema responsabile del computer relativo all'account. La nuova password dev essere inviata tramite posta interna o consegnata di persona.

Spiegazione/Note: gli account privilegiati hanno accesso a tutte le risorse di sistema e ai file che vi sono conservati. Naturalmente questi account hanno bisogno della massima protezione possibile.

Accesso remoto dell'assistenza esterna

Politica: nessuno dell'assistenza esterna (come i tecnici del fornitore di software o hardware) deve possedere tutte le informazioni sull'accesso remoto o essere autorizzato ad accedere a tutti i sistemi o macchinari correlati senza previa verifica dell'identità e autorizzazione a erogare questi servizi. Se il fornitore richiede un accesso privilegiato per garantire l'assistenza, la password dell'account usato sarà cambiata immediatamente una volta svolto il servizio.

Spiegazione/Note: gli intrusi informatici fingono di essere fornitori per accedere alle reti aziendali informatiche o di telecomunicazioni. Perciò è essenziale verificare l'identità del fornitore oltre all'autorizzazione a compiere qualsiasi lavoro sul sistema. Inoltre, le porte del sistema devono essere sbarrate una volta eseguito il lavoro cambiando la

password usata dal fornitore. Non dovrete permettere ad alcun fornitore di scegliersi la propria password, anche solo in via transitoria. Alcuni di loro sono noti per usare la stessa o simile presso più clienti. Per esempio, una compagnia specializzata nella sicurezza delle reti ha installato degli account privilegiati sui sistemi di tutti i clienti con la medesima password e, per aggiungere al danno la beffa, con l'accesso Telnet abilitato.

Autenticazione forte per l'accesso remoto ai sistemi aziendali

Politica: tutti i punti di connessione alla rete aziendale da localizzazioni remote devono essere protetti tramite l'uso di strumenti di autenticazione forte come le password dinamiche o la biometria.

Spiegazione/Note: molte imprese si basano sulle password statiche quale unico mezzo di autentica per gli utenti remoti. Questa abitudine è pericolosa in quanto poco sicura: gli intrusi informatici prendono di mira qualsiasi accesso remoto che possa rivelarsi l'anello debole della rete della vittima. Ricordatevi sempre che non sapete mai quando qualcun altro è al corrente della vostra password.

Quindi qualsiasi punto di accesso remoto dev'essere protetto con strumenti validi di autentica come identificatori a tempo, smart card o macchinari biometrici di modo che le password intercettate si rivelino inutili per l'attaccante.

Quando l'autentica basata su password dinamiche risulta poco pratica, gli utilizzatori dei computer devono rispettare religiosamente la politica di scegliere password difficili da indovinare.

Configurazione del sistema operativo

Politica: gli amministratori di sistema garantiranno che i sistemi operativi siano appena possibile configurati in modo da essere coerenti con tutte le relative procedure di sicurezza.

Spiegazione/Note: stilare e diffondere le politiche relative alla sicurezza è un passo fondamentale verso la riduzione dei rischi, ma nella maggior parte dei casi l'ottemperanza è per forza lasciata al singolo dipendente. Tuttavia ci sono tante contromisure informatiche che possono essere rese obbligatorie [illegible] del sistema per come la lunghezza obbligatoria de[illegible] le wolitiche di sicurezza tramite la configurazione dei parametri del sistema operativo sfila in maniera efficace la decisione dalle mani dell'elemento umano, accrescendo la complessiva sicurezza dell'organizzazione.

Cessazione obbligatoria

Politica: tutti gli account devono scadere dopo un anno.

Spiegazione/Note: l'intento di questa politica è di eliminare l'esistenza di account non più utilizzati, dato che gli intrusi informatici prendono normalmente di mira quelli in sonno. Questa procedura garantisce che tutti gli account appartenenti a ex dipendenti o incaricati rimasti indietro vengano disabilitati in automatico.

A discrezione della dirigenza potrete esigere che tutto il personale segua un corso di aggiornamento sulla sicurezza allo scadere del rinnovo oppure prenda in esame le procedure relative e firmi una lettera d'intesa.

Indirizzi generici di posta elettronica

Politica: il settore Information Technology approntera un indirizzo generico di e-mail per ogni dipartimento che comunica regolarmente con il pubblico.

Spiegazione/Note: l'indirizzo generico può essere diffuso al pubblico dal centralino o sul sito web aziendale. Altrimenti ogni dipendente potrà rivelare l'indirizzo personale di mail soltanto alle persone autorizzate.

Durante la prima fase di un attacco, l'ingegnere sociale di solito cerca di ottenere i numeri di telefono, i nomi e le cariche dei dipendenti. In quasi tutti i casi, queste informazioni sono a disposizione di chiunque sul sito web aziendale o banalmente telefonando. Se create caselle vocali generiche o indirizzi generici di e-mail renderete difficile associare il nome a un dato ufficio o responsabilità.

Informazioni per le registrazioni di dominio

Politica: quando ci si registra per ottenere un indirizzo Internet o per un nome dell'host, le informazioni riguardanti il personale amministrativo, tecnico o altro non devono identificare alcuna persona per nome. Invece dovreste presentare un indirizzo generico di e-mail e il numero telefonico principale dell'azienda.

Spiegazione/Note: lo scopo di questa politica è di impedire che un intruso informatico approfitti delle informazioni relative alle persone da interpellare. Quando si forniscono nomi e numeri di telefono, un intruso può utilizzarli per contattare le varie persone e tentare di convincerle con l'inganno a rivelare dati sul sistema o a eseguire azioni che lo aiuteranno nell'attacco. Oppure può fingersi una persona che figura nell'elenco per ingannare i colleghi. Invece di un indirizzo di e-mail di un dato dipendente, le informazioni per eventuali contatti devono essere in forma tipo amministratore@azienda.com.Il personale del settore telecomunicazionipuò fornire una casella vocale generica per i contatti amministrativi o tecnici al fine di limitare la rivelazione di informazioni utili per un attacco.

Installazione di aggiornamenti della sicurezza e del sistema operativo

Politica: tutti i patch di sicurezza per il sistema operativo e per le applicazioni saranno installati appena disponibili. Se questa politica si scontra con l'attività dei sistemi cruciali di produzione, questi aggiornamenti dovranno essere apportati appena possibile.

Spiegazione/Note: una volta identificato un punto debole, il produttore del software dovrebbe essere contattato immediatamente per sapere se è disponibile un patch o simili. Un sistema informatico privo di patch rappresenta una delle massime minacce alla sicurezza dell'impresa. Quando gli amministratori di sistema perdono tempo nell'applicazione degli aggiustamenti necessari, mantengono una finestra spalancata all'ingresso dell'attaccante. Ogni settimana su Internet sono identificate e pubblicate decine di punti deboli nella sicurezza. Fino a quando il personale della Information Technology non sarà metodico nell'applicazione di tutti i patch e correzioni riguardanti la sicurezza appena fattibile. la rete sarà sempre a rischio di incidenti nonostante questi sistemi si trovino dietro il firewall aziendale. È importantissimo essere al corrente delle vulnerabilità identificate nel sistema operativo oppure nelle applicazioni usate per il lavoro.

Informazioni sui siti web

Politica: il sito web aziendale esterno non rivelerà dettagli sulla struttura né identificherà per nome i dipendenti.

Spiegazione/Note: le informazioni sulla struttura quali gli organigrammi, le gerarchie, gli elenchi dipendenti, i nomi, le posizioni, i numeri di contatto interno, i numeri di matricola o simili usate per le procedure intramurali non dovrebbero essere disponibili sui siti web pubblici. Gli intrusi informatici ottengono spesso informazioni utilissime sul sito web del bersaglio, che poi manipoleranno per sembrare un dipendente informato nell'operazione del raggiro. Sarà più facile per loro sembrare credibili avendo in mano queste informazioni. Inoltre possono studiarle per scoprire quale può essere il bersaglio in possesso di o con accesso a informazioni di valore o cruciali.

Creazione di account privilegiati

Politica: non bisogna creare account privilegiati o garantire privilegi di sistema a un account se non dietro autorizzazione dell'amministratore o manager di sistema.

Spiegazione/Note: spesso gli intrusi informatici si fingono fornitori di hardware o software per ingannare il personale della Information Technology affinché crei account non autorizzati. Questa politica mira a bloccare simili attacchi garantendo un maggiore controllo sulla creazione di account privilegiati. Il manager o amministratore del sistema informatico deve approvare ogni richiesta di account con privilegi accresciuti.

Guest account

Politica: i guest account su qualsiasi sistema informatico o apparecchiature in rete devono essere disabilitati o eliminati, a parte un eventuale server FTP (File Transfer Protocol) con accesso anonimo abilitato approvato dalla direzione.

Spiegazione/Note: il guest account fornisce accesso temporaneo alle persone che non hanno bisogno di possedere un loro account fisso. Parecchi sistemi operativi vengono installati con un guest account abilitato in default. Invece dovrebbero essere sempre disabilitati visto che la loro esistenza viola il principio della responsabilità dell'utente. La IT dovrebbe essere in grado di rilevare ogni attività che coinvolga i computer e poterla riferire a uno specifico utente.

Gli ingegneri sociali non hanno molti problemi ad approfittarsi di questi account per ottenere accesso non autorizzato, sia direttamente sia convincendo persone autorizzate a usare un guest account.

Codifica dei dati di back-up esterni alla sede

Politica: ogni dato aziendale archiviato fuori sede dovrebbe essere cifrato per impedire l'accesso non autorizzato.

Spiegazione/Note: il personale operativo deve garantire che tutti i dati siano recuperabili nel caso occorra ripristinare le informazioni. Ciò richiede un test regolare fatto su un campione a caso di file cifrati per verificare che i dati possano essere recuperati. Inoltre, le chiavi usate per codificare i dati saranno conservate presso un gestore fidato nel caso in cui vadano perse o non siano disponibili.

Accesso dei visitatori alle connessioni di rete

Politica: tutti i punti di accesso Ethernet a portata di chiunque devono essere su una rete segmentata per impedire accesso non autorizzato alla rete interna.

Spiegazione/Note: questa politica è intesa a prevenire la connessione alla rete interna da parte di estranei nei locali dell'azienda. Le prese Ethernet installate nelle sale riunioni, in mensa, nei centri per la formazione o altre aree accessibili ai visitatori saranno filtrate per impedire l'accesso non autorizzato dei visitatori ai sistemi informatici aziendali. L'amministratore di rete o per la sicurezza può decidere di allestire una LAN virtuale in un commutatore, qualora possibile, per controllare l'accesso da questi punti.

Modem dial-in

Politica: i modem usati per le chiamate dial-in saranno impostati in modo da non rispondere prima del quarto squillo.

Spiegazione/Note: come spiegato nel film *War Games,* gli hacker usano una tecnica nota come "war-dialing" per localizzare le linee telefoniche con i modem collegati. La procedura inizia con l'attaccante che identifica i prefissi usati nella zona della compagnia bersaglio, poi usa un programma di scansione per provare tutti i numeri con quei prefissi, localizzando quelli che rispondono con un modem Per accelerare il processo, questi programmi sono configurati in modo di attendere solo uno o due squilli per vedere se risponde un modem prima di passare al numero successivo. Quando un'azienda imposta la risposta automatica sulle-linee modem su almeno quattro squilli, i programmi di scansione non le riconosceranno come tali.

Antivirus

Politica: ogni sistema informatico avrà installate e attivate le ultime versioni di programma antivirus.

Spiegazione/Note: per le imprese che non estendono gli antivirus e i pattern file (programmi che riconoscono i pattern classici dei virus per individuare quelli inediti) fino al livello delle scrivanie dei dipendenti, la responsabilità di installare e aggiornare il software sul proprio sistema, compresi i sistemi informatici usati per accedere in remoto alla rete aziendale, compete ai singoli utenti. Se fattibile, questo programma dev'essere impostato sull'aggiornamento automatico notturno delle configurazioni di virus e cavalli di Troia. Quando i pattern o signature file non sono allargati fino alle scrivanie dei dipendenti, compete al singolo utente del computer la responsabilità di aggiornarli almeno una volta alla settimana.

Queste misure si applicano su tutte le macchine e laptop usati per accedere ai sistemi informatici aziendali e valgono sia che il computer appartenga all'impresa o al singolo.

Allegati in arrivo (esigenze di elevata sicurezza)

Politica: in un'organizzazione con esigenze di alta sicurezza il firewall aziendale sarà configurato in modo da filtrare tutti gli allegati di posta elettronica.

Spiegazione/Note: questa politica vale solo per le imprese con esigenze elevate o per quelle che non hanno bisogno di ricevere allegati.

Autentica del software

Politica: tutti i nuovi programmi o adeguamenti o upgrade, che siano su supporto fisico o tramite Internet, devono essere autenticati prima dell'installazione. Questa politica è importante soprattutto per il settore Information Technology quando si installa un software che richiede privilegi di sistema.

Spiegazione/Note: il software cui ci si riferisce con questa politica comprende le componenti del sistema operativo, le applicazioni, i fix, i patch e gli aggiornamenti. Molti produttori di software hanno previsto metodi affinché il cliente possa controllare l'integrità della distribuzione, di solito tramite firma digitale. In ogni caso in cui l'integrità non può essere verificata, dovrete interpellare il produttore per verificare l'autenticità del programma.

Gli intrusi informatici sono noti per mandare a una vittima programmi presentati in modo che sembri essere stato il produttore ad averlo inviato. È essenziale verificare l'autenticità di ogni software che ricevete, soprattutto se non richiesto, prima di installarlo nei vostri sistemi.

Ricordate che un attaccante evoluto può sempre scoprire che avete ordinato un programma al produttore, e a quel punto può cancellare l'ordine, farsi arrivare il programma, modificarlo in modo da compiere funzioni impreviste e scorrette e inviarvelo nella confezione originale, dentro il cellofan se necessario. Una volta installato il prodotto, sarà in grado di controllarvi.

Password di default

Politica: tutti i sistemi operativi e i macchinari che all'inizio hanno una password di default devono cambiarla secondo la politica aziendale relativa.

Spiegazione/Note: molti sistemi operativi e apparecchi collegati al computer sono distribuiti con password di default, cioè con la stessa password abilitata su ogni unità venduta. Non cambiarla è un grave errore che mette a repentaglio l'azienda.

Le password di default sono notissime e reperibili nei siti web. Durante un attacco la prima password che l'intruso proverà sarà quella default del produttore.

Blocco dopo tentativi infruttuosi d'accesso (sicurezza media o bassa)

Politica: soprattutto nel caso di un'organizzazione con esigenze di sicurezza medie o basse, ogni volta che è stato fatto un dato numero di successivi tentativi falliti di log-in a un particolare account questo dev'essere bloccato per un certo lasso di tempo.

Spiegazione/Note: tutte le postazioni di lavoro di un'impresa e i suoi server devono essere impostati in modo da limitare il numero di tentativi falliti di entrata. Queste misure sono necessarie per impedire che si indovini la password a forza di tentativi, attacchi vocabolario o forza bruta per ottenere un accesso non autorizzato.

L'amministratore di sistema deve configurare le impostazioni di sicurezza in modo da bloccare un account appena la soglia desiderata di tentativi falliti è stata raggiunta. Si raccomanda che un account sia bloccato per almeno trenta minuti dopo sette tentativi.

Account disabilitati dopo tentativi d'accesso falliti (sicurezza elevata)

Politica: in un'organizzazione con esigenze di sicurezza elevate quando si raggiunge un dato numero di successivi tentativi falliti di log-in a un dato account questo dev'essere disabilitato fino al resettaggio da parte del gruppo responsabile dell'assistenza.

Spiegazione/Note: tutte le postazioni di lavoro e i server aziendali devono essere impostati in modo da limitare i tentativi falliti ravvicinati. Queste misure sono necessarie per impedire che si indovini la password a suon di tentativi, attacchi vocabolario o forza bruta per ottenere un accesso non autorizzato. L'amministratore di sistema deve configurare le impostazioni di sicurezza in modo da disabilitare l'account dopo cinque tentativi falliti. Dopo un attacco del genere il titolare dell'account dovrà chiamare l'assistenza tecnica per farselo abilitare. Prima di resettarlo, l'ufficio responsabile dovrà identificare il suo titolare seguendo le procedure di verifica e autorizzazione.

Cambiamento periodico delle password di account privilegiato

Politica: tutti i detentori di account privilegiato dovranno cambiare le loro password per lo meno ogni trenta giorni.

SpiegaziondNote: a seconda delle limitazioni del sistema operativo, l'amministratore dovrà far rispettare questa politica tramite la configurazione di parametri di sicurezza nel programma sistema.

Cambiamento periodico delle password utente

Politica: tutti i detentori di password dovranno cambiarle almeno ogni sessanta giorni.

Spiegazione/Note: nei sistemi operativi che forniscono questa opzione, l'amministratore di sistema deve far rispettare questa politica tramite la configurazione dei parametri di sicurezza nel programma.

Installazione di una nuova password di account

Politica: i nuovi account dovranno essere aperti con una password iniziale già scaduta, con la richiesta che il titolare scelga una nuova password appena comincia a utilizzarlo.

Spiegazione/Note: questa misura garantisce che il titolare sia il solo a conoscenza della sua password.

Password di riavvio

Politica: tutti i sistemi informatici devono essere configurati in modo da richiedere una password di riavvio.

Spiegazione/Note: i computer devono essere configurati in modo che all'accensione del computer occorra una password per avviare il sistema operativo, impedendo così che venga acceso e usato da persona non autorizzata. Questa politica vale per tutte le macchine della sede aziendale.

Esigenze delle password per gli account privilegiati

Politica: tutti gli account privilegiati devono avere una password forte, che deve:

- Non essere una parola reperibile in un vocabolario di qualsiasi lingua.

- Essere composta di maiuscole e minuscole con almeno una lettera, un simbolo e un numero.
- Essere lunga almeno dodici caratteri.
- Non avere alcuna relazione con l'azienda o con il singolo.

Spiegazione/Note: nella maggior parte dei casi gli intrusi informatici prendono di mira specifici account con privilegi. Ogni tanto l'attaccante sfrutterà altri punti deboli per ottenere il controllo del sistema. Le prime password che tenterà saranno le parole semplici e usate comunemente, reperibili in un vocabolario. Se scegliete password forti aumenterete la sicurezza riducendo le possibilità che un attaccante le trovi per tentativi, attacco vocabolario o forza bruta.

Punti d'accesso wireless

Politica: tutti gli utenti che accedono a una rete wireless devono usare la tecnologia WN (Virtual Private Network) a protezione della rete aziendale.

Spiegazione/Note: le reti wireless sono attaccabili con una nuova tecnica chiamata "war driving" che significa semplicemente girare in macchina o a piedi con un laptop provvisto di card 802.11B NIC fino a quando viene rilevata la rete wireless.

Molte aziende hanno impiantato reti wireless senza nemmeno attivare il WEP (Wireless Equivalency Protocol) che serve a rendere sicure le connessioni wireless tramite codifica. Ma anche quando attivata, l'attuale versione del WEP (mind-2002) non è abbastanza efficace: è già stata sprotetta e parecchi siti web sono impegnati a fornire i mezzi per localizzare i sistemi wireless aperti e per sproteggere i punti d'accesso abilitati dal WEP. Quindi è essenziale aggiungere un livello di protezione attorno al protocollo 802.11B usando la tecnologia WN.

Aggiornare i pattern file antivirus

Politica: ogni sistema informatico dev'essere programmato per aggiornare in automatico i pattern file antivirus e anti-Trojan.

Spiegazione/Note: come minimo questi aggiornamenti saranno settimanali. Nelle imprese in cui i dipendenti lasciano accesi i computer è caldamente raccomandato aggiornare i pattern file ogni notte.

Gli antivirus sono inefficaci se non sono aggiornati in modo da individuare ogni nuova forma di codice ostile. Dal momento che la minaccia di infezioni da virus, worm e cavalli di Troia aumenta notevolmente se i pattern file non vengono aggiornati è essenziale che gli antivirus e simili siano di ultima generazione.

Operazioni informatiche

Eseguire comandi o aprire programmi

Politica: il personale operativo informatico non deve eseguire comandi o aprire programmi su richiesta di persona non nota. Nei casi in cui una persona non verificata sembra avere un motivo valido per avanzare tale richiesta, quest'ultima non andrebbe esaudita senza la pregressa approvazione del dirigente.

Spiegazione/Note: i dipendenti del centro informatico sono i classici

bersagli degli ingegneri sociali dato che la loro posizione richiede di solito un account privilegiato e l'attaccante si aspetta che siano meno esperti delle procedure aziendali rispetto ai colleghi IT. Questa politica mira ad aggiungere un controllo adeguato per impedire che gli ingegneri sociali ingannino il personale operativo.

Lavoratori con account privilegiati

Politica: i dipendenti con account privilegiati non devono fornire assistenza o collaborazione ad alcuna persona non verificata. Questa nota si riferisce in particolare all'assistenza sulle macchine (come l'insegnamento all'uso delle applicazioni), all'accesso ai database aziendali, allo scaricamento di software o alla rivelazione dei nomi dei colleghi con diritto di accesso remoto.

Spiegazione/Note: spesso gli ingegneri sociali prendono di mira i dipendenti in possesso di account privilegiati. Questa politica mira a spingere il personale IT con account privilegiati a gestire con successo le chiamate che potrebbero corrispondere a un attacco.

Informazioni sui sistemi interni

Politica: il personale operativo informatico non deve mai diffondere informazioni relative ai sistemi informatici dell'azienda o agli apparecchi correlati senza avere prima identificato il richiedente.

Spiegazione/Note: spesso gli intrusi contattano gli operatori informatici per strappare informazioni preziose quali le procedure di accesso al sistema, i punti esterni di accesso remoto e i numeri di connessione che possono servire all'attaccante.

Nelle aziende che hanno un gruppo di assistenza tecnica, le richieste di informazioni sui sistemi o apparecchi correlati rivolte al personale del centro informatico dovrebbero essere considerate sospette. Ogni richiesta di informazioni dovrebbe essere vagliata in base alla politica aziendale di classificazione dei dati per decidere se il richiedente è autorizzato a detenere queste informazioni. Quando non è possibile decidere la classe delle informazioni, esse devono essere considerate a uso interno. In certi casi l'assistenza tecnica del fornitore dovrà essere in grado di comunicare con le persone che hanno accesso ai sistemi informatici aziendali. I fornitori dovranno rivolgersi a precisi contatti con il settore IT in modo da potersi conoscere di persona per una verifica più facile.

Rivelazione di password

Politica: gli operatori ai computer non devono mai rivelare la loro password o le altre loro affidate senza precedente approvazione del responsabile della Information Technology.

Spiegazione/Note: in generale la rivelazione di password a un'altra persona è severamente proibita. Questa politica riconosce che il personale operativo può avere necessità di rivelare una password a terzi in casi particolari. Questa eccezione alla politica generale richiede l'approvazione specifica di un caposettore. Per maggiore precauzione, la responsabilità di rivelare le informazioni autenticanti dovrebbe essere limitata a un gruppetto che ha ricevuto una speciale preparazione alle procedure di verifica.

Supporti elettronici

Politica: tutti i supporti elettronici contenenti informazioni non previste per la diffusione saranno tenuti sotto chiave in un posto fisicamente sicuro.

Spiegazione/Note: l'intento di questa politica è di impedire il furto fisico delle informazioni delicate contenute nei supporti elettronici.

Supporti di back-up

Politica: il personale operativo dovrebbe archiviare i supporti di back-up in una cassaforte aziendale o altro posto sicuro.

Spiegazione/Note: i supporti di back-up sono un altro bersaglio privilegiato degli intrusi informatici. Un attaccante non perderà tempo tentando di infiltrare un sistema informatico o una rete quando l'anello più debole della catena potrebbero essere i supporti di back-up non protetti. Una volta rubati questi, può compromettere la riservatezza dei dati conservati a meno che non siano cifrati. Perciò la protezione fisica di questi supporti è una misura fondamentale per preservare la riservatezza delle informazioni aziendali.

POLITICHE PER TUTTO IL PERSONALE

Che sia delle risorse umane o della IT, contabile o manutentore, ogni dipendente deve conoscere certe misure di sicurezza. Queste politiche si suddividono in misure generiche, uso dei computer, uso delle e-mail, telelavoro, uso dei telefoni, fax, caselle vocali e password.

Generiche

Riferire le telefonate sospette

Politica: i dipendenti che temono di essere stati oggetto di una violazione della sicurezza, comprese le richieste sospette di rivelare informazioni o eseguire azioni su una macchina, devono riferire immediatamente il fatto al gruppo segnalazione incidenti.

Spiegazione/Note: quando un ingegnere sociale non riesce a convincere il bersaglio a obbedire a una richiesta, ne cercherà sempre un altro. Riportando fatti o telefonate sospetti, un lavoratore compie il primo passo per la messa in stato d'allerta della compagnia per un attacco in corso. Quindi i singoli dipendenti sono la prima linea di difesa contro gli attacchi degli ingegneri sociali.

Documentare le telefonate sospette

Politica: nel caso di telefonata sospetta con le caratteristiche di un attacco, il dipendente si dovrà impegnare a strappare all'interlocutore i particolari che possano rivelare che cosa stia cercando, e prenderà nota per poter riferire in seguito.

Spiegazione/Note: questi dettagli possono aiutare a individuare o capire la traiettoria di un attacco una volta riferiti al gruppo segnalazione incidenti.

Rivelazione di numeri di modem

Politica: il personale non deve diffondere i numeri di telefono dei modem, ma riferire sempre queste richieste all'assistenza tecnica.

Spiegazione/Note: i numeri dei modem devono essere trattati come informazioni a uso interno, da dare solo ai dipendenti autorizzati per motivi di lavoro.

Di regola gli ingegneri sociali prendono di mira lavoratori o uffici che hanno capacità inferiori di proteggere le informazioni richieste. Per esempio, l'attaccante può telefonare alla contabilità fingendo di essere un dipendente dell'azienda telefonica con un problema di fatturazione e chiedere i numeri di fax o di connessione per risolvere quel problema. Spesso punta a quel dipendente che più difficilmente capirà il rischio insito nel rivelare queste informazioni o che non è addestrato alle politiche aziendali sulle informazioni.

Tesserini aziendali

Politica: tranne quando sono dentro il loro ufficio, tutti i dipendenti, compresa la dirigenza, devono indossare sempre il tesserino di riconoscimento.

Spiegazione/Note: tutti i lavoratori, compresa la dirigenza, dovrebbero essere preparati e motivati a capire che il tesserino è obbligatorio ovunque nei locali aziendali a parte l'ufficio specifico della persona e le aree aperte al pubblico.

Affrontare le violazioni all'uso del tesserino

Politica: tutti i dipendenti devono immediatamente bloccare ogni persona sconosciuta che non indossi il tesserino o il pass dei visitatori.

Spiegazione/Note: anche se nessuna azienda vuole creare un ambiente fatto di dipendenti con gli occhi sbarrati che cercano il modo per fregare un collega che si è avventurato in corridoio senza il tesserino, ugualmente ogni struttura interessata alla protezione delle informazioni deve prendere sul serio la minaccia di un ingegnere sociale che vaga indisturbato per l'azienda. I dipendenti dimostratisi diligenti nell'applicazione della politica del tesserino onnipresente devono essere gratificati con classici metodi come un articolo sul giornalino aziendale o in bacheca, qualche ora di permesso pagato oppure una lettera di raccomandazione nel loro fascicolo.

Andare a rimorchio (passaggio attraverso entrate protette)

Politica: i dipendenti che entrano in un edificio non devono permettere ad alcuno che non conoscano personalmente di seguirli (il cosiddetto "rimorchio") se, per entrare, hanno utilizzato uno strumento sicuro, come una tessera magnetica.

Spiegazione/Note: i dipendenti devono capire che non è segno di maleducazione richiedere alle persone ignote di identificarsi prima di aiutarle a entrare in una struttura o ad accedere a un'area sicura.

Gli ingegneri sociali usano spesso la tecnica nota come "rimorchio" in cui aspettano l'ingresso di una persona nella struttura o in un'area riservata per poi aggregarsi a lei, fingendo di essere legittimi colleghi. Un'altra classica tecnica di rimorchio è di portare degli scatoloni perché un lavoratore poco sospettoso gli apra la porta.

Distruzione di documenti delicati

Politica: i documenti delicati cartacei da eliminare devono essere tritati, e i supporti, compresi i dischi fissi, contenenti materiali o informazioni riservati devono essere distrutti secondo le misure proposte dal gruppo addetto alla sicurezza dei dati.

Spiegazione/Note: i tritadocumenti standard non distruggono come si deve i fogli, ma ci sono anche quelli che li riducono in poltiglia. La precauzione migliore è dare per scontato che la concorrenza andrà a frugare nel pattume in cerca di indizi preziosi.

Le spie industriali e gli attaccanti informatici ottengono sempre informazioni preziose dai materiali gettati nella spazzatura. In certi casi è risaputo che la concorrenza ha tentato di corrompere gli addetti alle pulizie per farsi consegnare il pattume. In un caso recente un dipendente della Goldman Sachs ha scoperto nella spazzatura materiali usati per una manovra di insider trading.

Identificatori personali

Politica: gli identificatori personali come il numero di matricola, quello della previdenza sociale, della patente, il luogo e data di nascita e il cognome da ragazza della madre non dovrebbero mai essere usati come mezzi per verificare l'identità. Non sono dati segreti e possono essere ottenuti in tanti modi.

Spiegazione/Note: un ingegnere sociale può procurarsi in qualche maniera gli identificato* altrui. E in pratica, contrariamente a ciò che pensa la gente, chiunque abbia una carta di credito e accesso a Internet è in grado di impossessarsene. Eppure, nonostante l'evidente pericolo, le banche, le aziende erogatrici di servizi e le compagnie di carte di credito ne fanno ampio uso. Questo spiega perché il furto di identità è il crimine a massimo tasso di crescita del decennio.

Organigrammi

Politica: i dettagli dell'organigramma aziendale non devono essere rivelati a chi non è dipendente.

Spiegazione/Note: le informazioni sulla struttura aziendale comprendono organigrammi, gerarchie, liste dipendenti di settore, nomi e posizioni dei dipendenti, numeri di contatto interno, numeri di matricola o simili. Nella prima fase di un attacco, il fine è sempre quello di raccogliere informazioni sulla struttura interna dell'azienda, dopodiché questi dati vengono usati per architettare un piano d'attacco. Inoltre, l'attaccante può analizzarli per scoprire quali dipendenti hanno accesso ai dati che sta cercando. Durante l attacco, le informazioni acquisite lo faranno sembrare un collega informato, rendendo più facile il raggiro della vittima.

Informazioni personali sui dipendenti

Politica: qualsiasi richiesta di informazioni personali sui dipendenti dev'essere segnalata alle risorse umane.

Spiegazione/Note: un'eccezione a questa politica potrebbe essere il numero di telefono di un dipendente che dev'essere rintracciato per problemi di lavoro o che è reperibile. Però è sempre preferibile farsi dare il numero di telefono del richiedente per farlo richiamare dall'interpellato.

Uso dei computer

Eseguire comandi su un computer

Politica: il personale non dovrebbe mai digitare comandi su un computer o su apparecchiature di rete, a meno che questi sia stato autorizzato come dipendente del settore Information Technology.

Spiegazione/Note: un trucco classico degli ingegneri sociali consiste nel richiedere a un diaendente di digitare un comando che cambia la configurazione del sistema, permettendo all'attaccante di accedere alla macchina della vittima senza autentica o di recuperare informazioni utilizzabili per un attacco tecnico.

Convenzioni interne sui nomi

Politica: i dipendenti non devono rivelare i nomi interni dei sistemi informatici o dei database senza una precedente verifica dell'appartenenza all'azienda di colui che ha fatto richiesta.

Spiegazione/Note: gli ingegneri sociali tenteranno talvolta di ottenere i nomi dei sistemi informatici aziendali. Appena scoperti questi nomi, l'attaccante telefona in azienda fingendosi un dipendente legittimo con problemi di accesso o di utilizzo di uno dei sistemi. Essendo al corrente del nome interno assegnato a quel dato sistema, apparirà più credibile.

Richieste di aprire programmi

Politica: il personale non deve mai aprire alcun programmi su richiesta di altri, salvo che non siano stati verificati come dipendenti del settore Information Technology.

Spiegazione/Note: qualsiasi richiesta di aprire programmi, applicazioni o eseguire azioni su una macchina dev'essere respinta a meno che il richiedente sia stato identificato come dipendente dell'IT. Se la richiesta coinvolge informazioni confidenziali tratte da file o messaggi elettronici, la risposta deve conformarsi alle procedure sulla diffusione delle notizie confidenziali. Vedi "Politica sulla diffusione di informazioni".

Gli attaccanti informatici convincono le vittime a eseguire programmi che permettono all'intruso di assumere il controllo del sistema. Quando un utente ignaro apre un programma piazzato da un attaccante, il risultato può essere l'accesso del malintenzionato ai sistemi informatici della vittima. Altri programmi registrano le attività dell'utente e rimandano queste informazioni all'attaccante. Come l'ingegnere sociale riesce a convincere una persona a eseguire istruzioni che possono essere dannose al computer, un attacco tecnologico convince il sistema operativo a eseguire istruzioni che possono causare altrettanto danno.

Scaricare o installare software

Politica: il personale non deve mai scaricare o installare software su richiesta di altri, a meno che il richiedente sia stato certificato come dipendente del settore IT.

Spiegazione/Note: i dipendenti dovrebbero drizzare le orecchie dopo ogni richiesta insolita che riguardi qualsiasi tipo di transazione con macchine informatiche. Una tattica classica degli ingegneri sociali prevede di ingannare le vittime inconsapevoli affinché scarichino e instal-

lino un programma che aiuterà l'attaccante a compromettere la sicurezza dei computer o della rete. In certi casi il programma può spiare in segreto l'utente oppure permettere all'attaccante di assumere il controllo del computer tramite l'utilizzo di un'applicazione nascosta di controllo remoto.

Password ed e-mail in chiaro

Politica: le password non saranno inviate per posta elettronica non crittata.

Spiegazione/Note: questa politica, anche se la sconsiglio, potrebbe essere tralasciata dai siti e-commerce in certe circostanze limitate, come

Inviare password ai clienti registrati sul sito.
Inviare password ai clienti che l'hanno persa o dimenticata.

Software di sicurezza

Politica: il personale non deve mai rimuovere o disabilitare antivirus e anti-Trojan, firewall e altri programmi di sicurezza senza previa approvazione del settore IT.

Spiegazione/Note: certe volte chi usa il computer disabilita il software di sicurezza senza necessità alcuna, pensando di rendere più veloce la macchina. Un ingegnere sociale potrebbe tentare di convincere un dipendente a disabilitare o rimuovere il software necessario per proteggere l'azienda dalle minacce alla sicurezza.

Installazione di modem

Politica: nessun modem dovrebbe essere collegato a una macchina fino ad approvazione del settore IT.

Spiegazione/Note: è importante sapere che i modem nelle postazioni di lavoro sono un gravoso problema per la sicurezza, soprattutto se collegati alla rete aziendale. Quindi questa politica serve a tenere sotto controllo le procedure di connessione dei modem.

Gli hacker usano il cosiddetto "war dialing" per identificare una linea modem attiva in un gruppo di numeri. La stessa tecnica può essere utilizzata per localizzare i numeri dei modem in un'azienda. Un attaccante può compromettere facilmente la rete aziendale se identifica un sistema collegato a un modem con un programma vulnerabile di accesso remoto, configurato con una password facile o addirittura nessuna.

Impostazioni modem e risposte automatiche

Politica: tutte le postazioni di lavoro con modem approvati dall'IT avranno l'opzione risposta automatica disattivata per impedire che qualcuno entri nel sistema informatico.

Spiegazione/Note: quando è fattibile, il settore IT dovrebbe fornire dei modem dial-out per i dipendenti che devono connettersi a sistemi esterni via modem.

Strumenti di cracking

Politica: i dipendenti non scaricheranno né useranno "tools" progettati per battere i meccanismi di protezione del software.

Spiegazione/Note: in Internet ci sono decine di siti dedicati ai programmi progettati per disattivare la protezione di shareware e software commerciali. L'uso di questi strumenti non solo viola i copyright del software ma è anche estremamente pericoloso. Visto che questi programmi provengono da fonti sconosciute, possono contenere codici ostili nascosti che potrebbero danneggiare un computer o installare un cavallo di Troia che permetterà all'autore del programma l'accesso alla macchina.

Postare online le informazioni

Politica: i dipendenti non riveleranno nessun dettaglio riguardo l'hardware o il software aziendale in nessun newsgroup pubblico, forum o BBS e non riveleranno le informazioni sui contatti se non in conformità con questa politica.

Spiegazione/Note: qualsiasi messaggio postato in Usenet, in forum online, BBS o mailing list può essere rintracciato per raccogliere dati sull'azienda o individuo bersaglio. Durante la fase di preparazione dell'attacco, l'ingegnere sociale può cercare in Internet i vari annunci che contengono informazioni utili sull'azienda, i suoi prodotti e le sue persone. Alcune affissioni contengono utilissimi frammenti di informazione che l'attaccante potrà sfruttare. Per esempio, un amministratore di rete può postare una domanda su come configurare i filtri su un particolare modello di firewall. Un attaccante che scopre quel messaggio, apprenderà informazioni preziose sul tipo e configurazione del firewall aziendale permettendogli di aggirarlo per accedere alla rete.

Questo problema sarà ridotto o evitato applicando una politica che consenta ai dipendenti di postare nei newsgroup da account anonimi he non) la struttura da cui provengono. Ovviamente dovete richieder ai endenti di non i e informazioni sui ntatti che possano identificare la struttura.

Floppy e altri supporti elettronici

Politica: se alcuni supporti usati per archiviare i dati dei computer, come i floppy o i CD-ROM, sono stati abbandonati in un'area di lavoro o su una scrivania, e sono di origine sconosciuta, non dovranno essere inseriti in una macchina.

Spiegazione/Note: un metodo di attacco usato per installare un codice ostile è quello di inserire dei programmi in un dischetto o CD-ROM etichettato in maniera stuzzicante (per esempio "Dati buste paga dipendenti – Confidenziale") e poi lasciarne varie copie nelle aree usate dai dipendenti. Se una singola copia viene inserita in un computer e si aprono i file che contiene, il codice ostile dell'attaccante sarà eseguito, creando una backdoor compromettente il sistema o causando altri danni alla rete.

Eliminazione dei supporti informatici

Politica: prima di gettare qualsiasi supporto contenente informazioni aziendali delicate, l'oggetto dovrà essere smagnetizzato per bene o danneggiato in maniera irrecuperabile persino se queste informazioni sono state cancellate.

Spiegazione/Note: se oggi è normale tritare i documenti su carta, il personale può invece trascurare la minaccia dei supporti elettronici

che hanno contenuto dati delicati e adesso sono da gettare. Gli attaccanti informatici tentano in tutti i modi di recuperare ogni dato archiviato su questi supporti. Forse l'impiegato può pensare che basti cancellare i file per essere sicuri che non siano più recuperabili, ma questo assunto è assolutamente errato e può provocare la caduta nelle mani sbagliate di informazioni aziendali confidenziali. Pertanto tutti i supporti elettronici che contengono o hanno contenuto informazioni non pubbliche devono essere cancellati o distrutti seguendo le procedure approvate dal gruppo designato.

Salvaschermo protetti da password

Politica: tutti coloro che usano il computer devono installare un salvaschermo con password e impostare il limite di stop dopo un certo periodo di inattività.

Spiegazione/Note: tutti i dipendenti sono responsabili dell'installazione della password salvaschermo e dello stop dopo più di dieci minuti di inattività. Questa politica è intesa a impedire che una persona non autorizzata utilizzi la macchina di quelia persona. Inoltre protegge i sistemi informatici aziendali dal facile accesso di estranei che siano riusciti a intrufolarsi nell'edificio.

Dichiarazione sulla rivelazione o condivisione delle password

Politica: prima di creare un nuovo account informatico, il dipendente o incaricato esterno deve firmare una dichiarazione scritta in cui riconosce di avere capito che le password non devono essere rivelate o condivise con nessuno, e afferma di accettare di ottemperare a questa politica.

Spiegazione/Note: l'accordo dovrebbe anche comprendere un codicillo secondo il quale la violazione di questo accordo può portare ad azioni disciplinari fino alla terminazione del rapporto.

Uso della posta elettronica

Allegati

Politica: gli allegati delle e-mail non devono essere aperti a meno che non siano attesi per lavoro o inviati da persona fidata.

Spiegazione/Note: tutti gli allegati devono essere esaminati attentamente. Potete esigere che sia data notizia preventiva da parte di una persona fidata dell'invio di un allegato, prima che il ricevente lo apra. In questo modo, ridurrete i rischi delle tattiche usate dagli ingegneri sociali per convincere le persone ad aprire gli attachment.

Un metodo per compromettere un sistema informatico è di convincere un dipendente ad aprire un programma ostile che crea un punto debole, fornendo accesso al sistema. Inviando un allegato di e-mail che ha un codice eseguibile o macro, l'attaccante può assumere il controllo del computer altrui. Un ingegnere sociale può inviare un allegato ostile, quindi chiamare per cercare di convincere il ricevente ad aprirlo.

Inoltro automatico a indirizzi esterni

Politica: l'inoltro automatico delle e-mail in arrivo a un indirizzo esterno è proibito.

Spiegazione/Note: questa politica è intesa a impedire che un esterno riceva le mail inviate a un indirizzo interno di posta elettronica. Ogni tanto i dipendenti impostano il forward delle e-mail che gli arrivano in ufficio a un indirizzo esterno quando sono assenti dal posto di lavoro. Oppure un attaccante può convincere un dipendente a impostare un indirizzo interno in modo che inoltri automaticamente a un indirizzo esterno all'azienda, facendosi poi passare come persona legittima in quanto facente parte della struttura dal momento che ha un indirizzo aziendale, convincendo così la gente a inviare a quell'indirizzo informazioni delicate per posta elettronica.

Inoltrare le e-mail

Politica: ogni richiesta proveniente da persona non identificata di inoltrare un messaggio di posta elettronica ad altra persona non identificata esige la verifica dell'identità del richiedente.

Verificare le e-mail

Politica: un messaggio di posta elettronica che sembra provenire da persona fidata e contiene una richiesta di fornire informazioni non classificate come pubbliche o di eseguire un'azione su un macchinario informatico necessita di un'ulteriore forma di autentica. Vedi "Procedure di verifica e autorizzazione".

Spiegazione/Note: un attaccante può falsificare facilmente un messaggio di e-mail e la sua intestazione facendolo apparire proveniente da un altro indirizzo di posta elettronica. Può anche inviare una e-mail da un sistema compromesso per fornire autorizzazioni false in modo da far rivelare informazioni o eseguire azioni. Persino esaminando l'intestazione di una e-mail non potete individuare i messaggi di posta elettronica inviati da un sistema interno compromesso.

*Utilizzo **dei** telefoni*

Partecipazione alle indagini telefoniche

Politica: i dipendenti non parteciperanno alle indagini telefoniche e non risponderanno ad alcuna domanda da parte di persona o organizzazione esterna. Tali richieste devono essere presentate alle relazioni pubbliche o ad altra persona delegata.

Spiegazione/Note: un metodo spesso usato dagli ingegneri sociali per ottenere informazioni preziose da utilizzare contro l impresa è di chiamare un dipendente sostenendo di essere impegnati in un'inda ine di mercato. È incredibile quante persone sono felici di fornire informazioni sull'azienda e su se stesse a estranei credendoli impegnati in una ricerca legittima. Tra le domande innocue, colui che telefona inserirà qualche quesito cui vuole risposta. Alla fine, queste informazioni saranno usate per compromettere la rete aziendale.

Rivelazione dei numeri di telefono interni

Politica: se una persona non identificata chiede a un dipendente il suo numero questi potrà decidere in maniera ponderata se è necessario nell'ambito della strategia aziendale.

Spiegazione/Note: questa politica mira a esigere che i dipendenti de-

cidano in maniera ponderata se sia necessario rivelare il loro interno. Quando trattano con persone che non hanno dimostrato una vera necessità di conoscere quel numero la scelta più sicura è chiedergli di telefonare al centralino per farsi passare l'interno.

Password nelle caselle vocali

Politica: lasciare messaggi contenenti informazioni sulle password nella segreteria o casella vocale di qualcuno è proibito.

Spiegazione/Note: spesso un ingegnere sociale accede alla casella vocale di un dipendente perché non è adeguatamente protetta per colpa di un codice facile da indovinare. Un sofisticato intruso informatico può creare la sua propria falsa casella vocale convincendo un altro dipendente a lasciare un messaggio contenente informazioni sulla password. Questa politica sconfigge una trovata del genere.

Uso del fax

Inoltrare fax

Politica: nessun fax può essere ricevuto e inoltrato a una terza parte senza verifica dell'identità del richiedente.

SpiegaziondNote: i ladri di informazioni possono convincere dipendenti fidati a faxare informazioni delicate a una macchina sita nei locali aziendali. Prima di dare quel numero alla vittima, l'attaccante telefona a un dipendente ignaro, come una segretaria, e le chiede di poter faxare un documento che passerà a prendere dopo. In seguito, quando la segretaria ignara riceve il fax, l'attaccante le telefona e chiede che quel documento sia spedito in un altro posto, casomai sostenendo che serve per una riunione urgente. Visto che la persona cui si chiede di rimbalzare il fax di solito non è al corrente del valore dell'informazione obbedirà alla richiesta.

Verifica delle autorizzazioni per fax

Politica: prima di eseguire le istruzioni ricevute per facsimile, il mittente dev'essere verificato come dipendente o altra persona fidata. Di solito, basta una telefonata al mittente per verificare la richiesta.

SpiegaziondNote: i dipendenti devono essere cauti con le richieste insolite ricevute per fax, come quella di eseguire comandi su un computer o rivelare informazioni. I dati nell'intestazione di un documento faxato possono essere falsificati cambiando le impostazioni della macchina mittente. Perciò l'intestazione di un fax non dev'essere accettata come mezzo di identificazione o autorizzazione.

Invio di informazioni delicate per fax

Politica: prima di inviare informazioni delicate per fax a una macchina collocata in un'area accessibile ad altro personale, il mittente spedirà una pagina di copertina. Appena giunta, il ricevente spedirà una pagina di risposta per dimostrare di essere fisicamente presente presso la macchina. A quel punto il mittente invierà il fax.

SpiegaziondNote: questa procedura tipo stretta di mano garantisce al mittente che il ricevente è presente fisicamente all'altro capo. Inoltre

verifica che il numero di telefono dell'altra macchina non abbia il trasferimento di chiamata in altra sede.

Invio per fax di password

Politica: le password non devono essere inviate per facsimile in alcun caso.

Spiegazione/Note: Inviare informazioni di autentica per fax non è sicuro. Quasi tutti i fax sono accessibili a molti dipendenti, e inoltre si basano sulla rete telefonica pubblica manipolabile in modo da trasferire la chiamata all'attaccante presso un altro numero.

Uso caselle vocali

Password delle caselle vocali

Politica: le password delle caselle vocali non devono essere mai rivelate a nessuno per nessun motivo. Inoltre, devono essere cambiate ogni novanta giorni o anche meno.

Spiegazione/Note: le informazioni aziendali confidenziali possono finire nei messaggi delle caselle vocali, perciò per proteggerle i dipendenti devono cambiare spesso la password della casella vocale senza mai rivelarla. Inoltre, chi usa questo tipo di segreteria non deve utilizzare le stesse password o simili nell'arco di dodici mesi.

Password su più sistemi

Politica: gli utenti di casella vocale non devono usare la stessa password in un altro sistema telefonico o informatico, che sia dentro o fuori l'azienda.

Spiegazione/Note: l'uso di password simili o identiche per più apparecchi, come la casella vocale o il computer, rende più facile all'ingegnere sociale indovinare tutte le password di un utente dopo avere trovato la prima.

Impostare le password della casella vocale

Politica: gli utenti e l'amministratore delle caselle vocali devono creare una password difficile da indovinare, che non avrà alcun rapporto con la persona o l'azienda né seguirà uno schema facile da indovinare.

Spiegazione/Note: le password non devono contenere numeri sequenziali o ripetitivi (per es., **1111, 1234, 1010**), non devono essere il numero dell'interno telefonico o essere basate su di esso né avere alcun rapporto con indirizzo, codice d'avviamento postale, data di nascita, targa, telefono, peso, Q.I. o altre informazioni prevedibili.

Messaggi "vecchi"

Politica: quando i messaggi di posta vocale mai sentiti non sono indicati come nuovi, l'amministratore dev'essere avvertito di una possibile violazione della sicurezza e la password sarà immediatamente cambiata.

Spiegazione/Note: gli ingegneri sociali possono accedere in vari modi a una casella vocale. Il dipendente che si accorge che i messaggi mai

ascoltati non sono annunciati come nuovi deve dare per scontato che un'altra persona abbia ottenuto accesso non autorizzato alla casella vocale e ascoltato quei messaggi.

Saluti esterni

Politica: il personale limiterà la rivelazione di informazioni nei saluti che vanno all'esterno sulla propria casella vocale. Di regola non bisogna diffondere le informazioni relative alle mansioni quotidiane o al programma delle trasferte.

Spiegazione/Note: i saluti esterni (a persone fuori dalla struttura) non comprenderanno cognome, interno o motivo dell'assenza (tipo viaggio, programma vacanze o itinerario giornaliero). Un attaccante potrebbe usarle per architettare una storia plausibile per ingannare altri dipendenti.

Schemi delle password

Politica: gli utenti di casella vocale non sceglieranno una password una cui parte rimane fissa mentre un'altra cambia secondo uno schema prevedibile.

Spiegazione/Note: per esempio, non usate una password come **743501,743502,743503** ecc., in cui gli ultimi due numeri corrispondono al mese in corso.

Informazioni confidenziali o personali

Politica: le informazioni confidenziali o personali non devono essere diffuse come messaggi di casella vocale.

Spiegazione/Note: il sistema telefonico aziendale è notoriamente più vulnerabile di quello informatico. Di solito le password sono una serie di cifre, il che limita in maniera notevole il numero di possibilità che un attaccante deve indovinare. Inoltre in certe organizzazioni le password delle caselle vocali possono essere condivise con segretari e altri collaboratori incaricati di raccogliere i messaggi per il loro superiore. Sapendo ciò, nessuna informazione delicata dev'essere lasciata su una casella vocale.

Password

Sicurezza telefonica

Politica: le password non saranno in alcun caso rivelate per telefono.

Spiegazione/Note: gli attaccanti possono trovare la maniera di ascoltare una conversazione telefonica sia di persona sia attraverso un'apparecchiatura.

Rivelare le password dei computer

Politica: in nessun caso chi usa un computer rivelerà la password per un qualsiasi motivo senza previo consenso scritto del responsabile dell'IT.

Spiegazione/Note: lo scopo di tanti attacchi è quello di indurre le persone ignare a rivelare username e password, e questa politica introduce un

passo cruciale verso la riduzione del rischio di attacchi fortunati contro l'azienda. Quindi va rispettata religiosamente in tutti i settori.

Password di Internet

Politica: il personale non deve mai usare in un sito Internet una password identica o simile a quella che usa su un qualsiasi sistema aziendale.

Spiegazione/Note: gli operatori di sito web con meno scrupoli allestiscono un sito che offre qualcosa o promette un premio. Per registrarsi il visitatore del sito deve inserire indirizzo di e-mail, username e password. Visto che tanti usano a ripetizione le stesse informazioni, l'operatore poco scrupoloso tenterà di usare questa password e le sue varianti per attaccare il sistema informatico del bersaglio sia a casa sia in ufficio. Il computer di lavoro del visitatore può essere talvolta identificato tramite l'indirizzo e-mail inserito durante la procedura di registrazione.

Password su più sistemi

Politica: il personale non deve mai usare in più di un sistema una password identica o simile. Questa politica vige per vari tipi di macchina (computer o casella vocale), varie collocazioni (a casa o in ufficio) e vari tipi di sistema, apparecchiatura (router o firewall) o programma (database o applicazione).

Spiegazione/Note: gli attaccanti fanno leva sulla natura umana per entrare nei sistemi e nelle reti. Sanno che per evitare il disturbo di ricordare più password tanti usano la medesima o simile su ogni sistema in cui accedono. Quindi l'intruso tenterà di scoprire la password di un sistema in cui il bersaglio ha un account e una volta ottenutala è assai probabile che quella o una sua variante daranno accesso ad altri sistemi o apparecchi usati dal dipendente.

Riutilizzo delle password

Politica: nessun computer userà la stessa password o simili nell'arco di diciotto mesi.

Spiegazione/Note: anche se un attaccante scopre una password, il cambio frequente minimizzerà i danni che può infliggere. Una nuova password diversissima dalle precedenti rende più difficile indovinarla.

Struttura delle password

Politica: i dipendenti non devono scegliere una password in cui una parte rimane fissa e un altro elemento cambia secondo uno schema prevedibile.

Spiegazione/Note: per esempio non usate una password come Kevin01, Kevin02, Kevin03 ecc., in cui gli ultimi due numeri corrispondono al mese corrente.

Scegliere le password

Politica: chi usa il computer dovrebbe creare o scegliere una password che rispetti le seguenti esigenze. Deve:

- Essere lunga almeno 8 caratteri per gli account standard e almeno 12 per gli account privilegiati.
- Contenere almeno un numero, un simbolo (come $, _, !, &), almeno una minuscola e una maiuscola (ammesso che queste variabili siano lette dal sistema operativo).
- Non essere una delle seguenti voci: parola di vocabolario in qualsiasi lingua, parola collegata alla famiglia, hobby, veicolo, lavoro, targa, numero della previdenza sociale, indirizzo, telefono, nome dell'animale domestico, compleanno o frasi composte dalle parole suddette.
- Non essere una variante di una Password già usata, con un elemento che rimane lo stesso e un altro che cambia, come kevin1, kevin2 o kevingen, kevinfeb.

Spiegazione/Note: i parametri sopraelencati vi forniranno una password difficile da indovinare. Un'altra possibilità è il metodo vocali-consonanti che fornisce una password pronunciabile e facile da ricordare. Per ottenere questo genere di parola d'ordine basta sostituire una consonante a ogni C e una vocale a ogni V della seguente griglia CVCVCVCV. Per esempio MMOCASO, CUSOJENA.

Appuntare le password

Politica: il personale deve appuntare le password soltanto quando le conserva in un posto sicuro lontano dal computer o da altra macchina protetta dalla suddetta parola d'ordine.

Spiegazione/Note: i dipendenti devono essere scoraggiati dall'appuntare le password. Però in certi casi può essere necessario, per esempio quando un lavoratore ha più account su diversi sistemi. Ogni password scritta va conservata in un posto sicuro lontano dal computer. In nessun caso può essere lasciata sotto la tastiera o attaccata allo schermo.

Password in chiaro nei *file*

Politica: le password in chiaro non saranno registrate in alcun file né conservate come testo richiamabile premendo un tasto funzione. Se necessario, possono essere registrate usando un crittaggio approvato dal settore IT per impedire rivelazioni non autorizzate.

Spiegazione/Note: le password possono essere facilmente recuperate da un attaccante se conservate in forma non cifrata nei file del computer, nei patch, nei tasti funzione, nei file di log-in, in programmi macro o di script o altri che contengano password a siti FTP.

Politiche per il telelavoro

Il telelavoro avviene fuori dal firewall aziendale, ed è perciò più vulnerabile. Queste misure vi aiuteranno a impedire che gli ingegneri sociali usino i dipendenti in telelavoro come porta aperta sui vostri dati.

Thin client

Politica: tutto il personale autorizzato a collegarsi in accesso remoto userà un "thin client" per connettersi alla rete aziendale.

Spiegazione/Note: quando un attaccante studia la strategia, cerca

sempre di identificare gli utenti che accedono dall'esterno alla rete aziendale. Perciò chi è in telelavoro è il primo bersaglio. È meno probabile che i loro computer godano di controlli severi, quindi possono essere l'anello debole che compromette l'intera rete.

Qualsiasi computer che si collega a una rete fidata può essere zavorrato con logger delle digitazioni oppure la connessione autenticata può essere dirottata. In questi casi una strategia "thin client" può risolvere i problemi. Un thin client è simile a un dumb terminal o a una postazione di lavoro senza disco. Il computer remoto non può registrare, e il sistema operativo, le applicazioni e i dati si troveranno tutti nella rete aziendale. L'accesso alla rete in thin client riduce il rischio di sistemi non aggiornati e non corretti e di codici ostili. Insomma, centralizzando i controlli la gestione della sicurezza del telelavoro è più efficace e più facile. Piuttosto che basarsi sull'inesperto telelavoratore sperando che gestisca in modo adeguato i problemi della sicurezza, adesso queste responsabilità riposano sulle spalle degli amministratori di sistema, rete o sicurezza, cioè di persone più preparate.

Software di sicurezza per i sistemi informatici in telelavoro

Politica: qualsiasi sistema informatico usato per collegarsi alla rete aziendale deve avere antivirus, anti-Trojan e un firewall personale (hardware o software). I pattern file antivirus o anti-Trojan devono essere aggiornati almeno una volta alla settimana.

Spiegazione/Note: di solito i telelavoratori non sono preparati sui temi della sicurezza e possono per negligenza o distrazione lasciare aperto a un attacco il loro sistema e la rete aziendale. Perciò pongono un serio rischio alla sicurezza se non sono adeguatamente preparati. Oltre a installare antivirus e anti-Trojan per proteggersi da codici ostili, sarà necessario un firewall per impedire a qualsiasi utente malintenzionato di accedere a un servizio abilitato sul sistema del telelavoratore.

Il rischio di quando non si usano le tecnologie minime di sicurezza per impedire che un codice ostile si propaghi non può essere sottovalutato, come dimostra un attacco sferrato alla Microsoft. Un sistema informatico di un telelavoratore della Microsoft usato per connettersi alla rete dell'azienda è stato infettato da un cavallo di Troia. Gli intrusi sono riusciti a sfruttare la sua connessione fidata alla rete sviluppo della Microsoft per rubare un codice sorgente.

Politiche per le risorse umane

Il dipartimento risorse umane è incaricato di proteggere i dipendenti da chi tenta di scoprire le informazioni personali in ufficio e anche di proteggere l'azienda dai licenziati vendicativi.

Politica: ogni volta che un dipendente si dimette o è licenziato, le risorse umane devono immediatamente:

- Toglierlo dall'elenco telefonico online e disattivare o passare ad altri la sua casella vocale.
- Notificare il cambiamento al personale all'entrata o nell'atrio.
- Aggiungere il suo nome all'elenco partenze che sarà inviato per posta elettronica a tutto il personale almeno una volta alla settimana.

Spiegazione/Note: i dipendenti appostati agli ingressi devono essere awertiti affinché impediscano che l'ex dipendente rientri nei locali. Inoltre la notifica al resto del personale evita che l'ex si faccia passare per dipendente attivo convincendo altri a commettere azioni dannose per la struttura. In certi casi può essere necessario richiedere a ogni utente del suo ex ufficio di cambiare le password. (Quando sono stato licenziato dalla GTE solo per colpa della mia fama di hacker, l'azienda ha chiesto a tutto il personale di cambiare la password.)

Notifica al settore IT

Politica: quando un dipendente se ne va o è licenziato, le risorse umane dovrebbero avvertire immediatamente la Information Technology perché disabiliti i suoi account, compresi quelli di accesso ai database, modem o Internet.

Spiegazione/Note: è essenziale disattivare immediatamente ogni accesso di ex dipendente a tutti i sistemi informatici, apparecchi di rete, database o altre macchine attinenti ai computer. Altrimenti l'azienda lascerà la porta aperta al rancoroso perché acceda ai sistemi informatici provocando grossi danni.

Informazioni confidenziali usate durante la procedura di assunzione

Politica: gli annunci e le altre modalità per sollecitare gli eventuali candidati ai posti di lavoro vacanti dovrebbero evitare il più possibile di identificare il software e l'hardware usati dall'azienda.

Spiegazione/Note: i responsabili e il personale delle risorse umane dovrebbero rilasciare sull'hardware e software aziendale soltanto le informazioni necessarie per il curriculum dei candidati con precise qualifiche. Gli intrusi informatici leggono i giornali e i comunicati stampa e visitano i siti Internet in cerca di annunci di lavoro. Spesso le aziende rilasciano troppe informazioni sui tipi di programmi e macchine che usano, visto che serve per attirare i candidati giusti. Una volta che l'intruso è al corrente di questi sistemi è pronto per la successiva fase dell'attacco. Per esempio, sapendo che una data azienda usa il sistema operativo VMS può fare una telefonata pretesto per capire di quale versione si tratta e poi inviare un patch falso che sembri arrivare dal produttore del software. Una volta installato il patch, l'attaccante potrà entrare.

Informazioni personali dei dipendenti

Politica: il settore risorse umane non deve mai diffondere informazioni personali su dipendenti attuali o passati, incaricati esterni, consulenti, awentizi o stagisti, se non dietro consenso scritto del dipendente o del responsabile delle risorse umane.

Spiegazione/Note: i cacciatori di teste, gli investigatori privati e i ladri di identità prendono di mira le informazioni personali quali i numeri di matricola, della previdenza sociale, la data di nascita, le buste paga, i dati finanziari come i saldi dei conti correnti e quelli sul piano assistenza medica. L'ingegnere sociale può impossessarsi di queste informazioni per farsi passare per la tal persona. Anche i nomi dei neoassunti possono rivelarsi estremamente preziosi per i ladri di informazioni. I nuovi assunti sono più propensi a obbedire a una richiesta di per-

sona con maggiore anzianità o in posizione più elevata o da parte di uno che sostiene di essere della sorveglianza.

Controlli sul passato

Politica: un controllo sul passato è necessario per ogni nuovo assunto, incaricato, consulente, lavoratore a tempo determinato o stagista prima di offrirgli il posto o avviare un rapporto a contratto.

Spiegazione/Note: per motivi di costo questa misura di verifica può essere limitata ad alcune cariche fidate. Ricordate però che qualsiasi persona che ha accesso agli uffici può essere pericolosa in potenza. Per esempio, gli addetti alle pulizie possono entrare negli uffici e quindi accedere ai computer. Un attaccante, in grado di mettere le mani su un computer, può installare un logger per le digitazioni in meno di un minuto, catturando così le password.

Ogni tanto, gli intrusi informatici si spingono fino a farsi assumere per accedere ai sistemi e alle reti dell'azienda bersaglio. Un attaccante può ottenere facilmente il nome della ditta incaricata delle pulizie chiamando il responsabile presso l'azienda bersaglio e sostenendo di essere di una ditta di pulizie concorrente, facendosi così dare il nome di chi sta fornendo in quel momento il servizio.

Politiche per la sicurezza fisica

Anche se gli ingegneri sociali evitano di farsi vedere in carne e ossa sul posto di lavoro che vogliono colpire, certe volte violeranno il vostro spazio. Queste misure vi aiuteranno a tenere i vostri locali al sicuro da questa minaccia.

Identificazione dei non dipendenti

Politica: i fattorini delle consegne e gli altri esterni che devono accedere ai locali aziendali con regolarità devono possedere un tesserino speciale o un altro identificatore in conformità con la politica decisa dalla sorveglianza.

Spiegazione/Note: dovrete rilasciare una forma di tesserino all'uopo ai non dipendenti che devono entrare nell'edificio con regolarità (per esempio per le consegne di cibi e bevande alla mensa o per riparare fotocopiatrici o installare telefoni). Gli altri che devono entrare ogni tanto o per una volta sola saranno trattati come visitatori e scortati per tutto il tempo.

Identificazione dei visitatori

Politica: tutti i visitatori devono presentare un documento d'identità valido se vogliono essere ammessi nei locali.

Spiegazione/Note: il personale della sorveglianza o dell'accoglienza dovrebbe fare una fotocopia del documento d'identità prima di rilasciare un pass visitatore. Questa copia dovrebbe essere conservata assieme al registro visitatori. Altrimenti la guardia o il receptionist può vrendere nota sul registro. Non saranno comunque i visitatori a inserire le informazioni sulla loro identità. Gli ingegneri sociali, che cercano di accedere a un edificio scriveranno sempre informazioni false sul registro. Sebbene non sia difficile ottenere documenti contraffatti e im-

parare il nome di un dipendente che si sostiene di andare a trovare, un responsabile che registra l'ingresso aggiunge un livello di sicurezza alla procedura.

Scortare i visitatori

Politica: i visitatori vanno scortati o accompagnati per tutto il tragitto da qualcuno del personale.

Spiegazione/Note: un classico trucco degli ingegneri sociali prevede di organizzare una visita a un dipendente dell'azienda (per esempio a un tecnico della produzione con la scusa di essere dipendente di un partner strategico). Dopo essere stato accompagnato all'incontro iniziale, l'ingegnere sociale garantisce al suo ospite che sa trovare l'uscita da solo, dopodiché sarà libero di aggirarsi nell'edificio e casomai accedere a informazioni delicate.

Tesserini temporanei

Politica: il personale di un'altra sede che non ha con sé il tesserino deve presentare un documento d'identità valido perché gli sia rilasciato un pass temporaneo.

Spiegazione/Note: spesso per entrare gli attaccanti si fingono colleghi di un altro ufficio o filiale dell'azienda.

Evacuazione di emergenza

Politica: in una situazione di emergenza o durante un'esercitazione, il personale della sorveglianza deve verificare che tutti abbiano lasciato i locali.

Spiegazione/Note: il personale della sorveglianza deve controllare tutti i ritardatari rimasti nei bagni o negli uffici. In base alle autorizzazioni dei vigili del fuoco o delle altre autorità responsabili della crisi, le forze di sorveglianza devono controllare chiunque lasci l'edificio parecchio tempo dopo l'evacuazione. Le spie industriali e gli intrusi informatici evoluti possono provocare una diversione per accedere a un edificio o area sicura. Una diversione utilizzata di frequente è di spandere nell'aria una sostanza innocua nota come butil ercaptano per dare l'impressione che ci sia una fuga di gas. Appena il personale inizia la procedura di evacuazione l'attaccante ardito sfrutta la diversione o per rubare informazioni oppure per accedere ai sistemi informatici aziendali. Un'altra tattica tipica dei ladri di informazioni prevede di indugiare, certe volte in un bagno o in un ripostiglio, quando è prevista un'esercitazione di evacuazione o dopo aver innescato un fumogeno o un altro aggeggio che faccia scattare l'evacuazione di emergenza.

Visitatori nella stanza della posta

Politica: nessun visitatore potrà accedere alla stanza della posta senza la supervisione di un dipendente dell'azienda.

Spiegazione/Note: questa politica è intesa a impedire che un estraneo scambi, invii o rubi posta intraziendale.

Targhe

Politica: se l'azienda ha un parcheggio custodito, il personale della sorveglianza registrerà le targhe all'ingresso di ogni veicolo.

Cassonetti

Politica: i cassonetti dovranno sempre rimanere sul suolo aziendale ed essere inaccessibili al pubblico.

Spiegazione/Note: hacker e spie industriali possono ottenere informazioni di valore dai bidoni di un'azienda. Alcune sentenze hanno sancito che la spazzatura è una proprietà abbandonata, perciò la cosiddetta "pesca nei cassonetti" è assolutamente legale finché i contenitori sono su suolo pubblico. Perciò è importante che i cassonetti rimangano su suolo aziendale, dove la compagnia ha diritto di proteggere i bidoni e il loro contenuto.

Politiche per il personale dell'accoglienza

I receptionist costituiscono spesso la linea avanzata quando si tratta di affrontare gli ingegneri sociali, eppure non forniamo loro un sufficiente training in modo che siano in grado di riconoscere e bloccare un intruso. Prevedete queste politiche per aiutare i vostri addetti all'accoglienza a proteggere l'azienda e i suoi dati.

Elenco interno

Politica: la diffusione delle informazioni contenute nell'elenco interno va limitata alle persone impiegate dall'azienda.

Spiegazione/Note: tutte le cariche, nomi, numeri di telefono, indirizzi contenuti nell'elenco aziendale dovrebbero essere considerate informazioni interne e diffuse solo in ottemperanza alla politica relativa alla classificazione dei dati e alle informazioni a uso interno.

Inoltre ogni persona che chiama deve avere già il nome o il numero d'interno di colui che cerca. Anche se il centralinista o addetto al banco può passare un singolo quando chi chiama non conosce l'interno, dovrebbe essere proibito rivelare di quale numero si tratta. (Ai curiosoni consiglio di verificare questa procedura chiamando un qualsiasi ente pubblico e chiedendo al centralinista di rivelare un numero d'interno.)

Numeri di telefono di specifici uffici/dipartimenti

Politica: il personale non deve mai dare i numeri diretti del servizio assistenza, del settore telecomunicazioni, della sala operativa computer o degli amministratori di sistema senza avere prima verificato che il richiedente abbia legittimo bisogno di contattarli. Il centralinista deve annunciare chi c'è al telefono quando trasferisce una chiamata a questi gruppi.

Spiegazione/Note: anche se alcune organizzazioni troveranno sin troppo restrittiva questa politica, essa rende più difficile agli ingegneri sociali spacciarsi come dipendente convincendo un presunto collega a trasferire la telefonata a quell'interno (che in certi sistemi fa sembrare la chiamata interna all'azienda) oppure dimostrando di conoscere i numeri di interno per ammantarsi di un'aura di autenticità.

Rimbalzare informazioni

Politica: gli operatori telefonici e i receptionist non devono accettare messaggi o passare informazioni per conto di altri non direttamente noti a un altro dipendente attivo.

Spiegazione/Note: gli ingegneri sociali sono abilissimi a fare in modo che i dipendenti garantiscano per la loro identità. Un trucco classico è di ottenere il numero del banco nell'atrio e con un pretesto chiedergli di accettare i messaggi che possono arrivare a nome loro. Poi, durante una telefonata alla vittima, fingeranno di essere un collega, chiederanno un'informazione delicata o di fare qualcosa, quindi daranno come numero cui richiamare quello del banco. In seguito richiameranno il receptionist per farsi dare il messaggio lasciato per loro dalla vittima candida.

Oggetti lasciati per il ritiro

Politica: prima di consegnare un oggetto a un fattorino o altra persona non verificata, il receptionist o il guardiano dovranno chiedere un documento di riconoscimento e inserire l'informazione nel registro dei ritiri come richiesto dalle procedure approvate.

Spiegazione/Note: una tattica degli ingegneri sociali prevede che un dipendente affidi materiali delicati a un collega in teoria autorizzato lasciandoli al banco d'accoglienza per il ritiro. Ovviamente l'addetto all'accoglienza o la guardia presume che il pacchetto sia stato approvato da chi di dovere. L'ingegnere sociale passerà a prenderlo di persona oppure userà un fattorino.

Politiche per il gruppo segnalazione incidenti

Ogni azienda dovrebbe istituire un gruppo centralizzato da awertire tutte le volte che si rileva una qualche forma di attacco alla sicurezza aziendale. Quelle che seguono sono le linee di condotta per avviare e strutturare le attività di questo gruppo.

Gruppo segnalazione incidenti

Politica: un individuo o gruppo sarà delegato a questo scopo e i dipendenti saranno istruiti a segnalare loro gli incidenti attinenti alla sicurezza dei dati. Tutto il personale sarà provvisto delle informazioni di contatto per il gruppo.

Spiegazione/Note: i dipendenti devono imparare come identificare una minaccia alla sicurezza ed essere preparati ad avvisare un preciso gruppo segnalazione incidenti. È anche importante che l'organizzazione preveda procedure e competenze specifiche per come interverrà il gruppo alla segnalazione di una minaccia.

Attacchi in corso

Politica: ogni volta che il gruppo segnalazione incidenti riceve denunce di attacco in corso avvierà immediatamente le procedure per avvisare tutti i dipendenti dei gruppi presi di mira.

Spiegazione/Note: il gruppo segnalazione incidenti o il responsabile dovrebbero anche decidere se lanciare un'allerta in tutta l'azienda. Una volta che il responsabile o il gruppo si convince che è in corso un attacco la priorità dev'essere la minimizzazione del danno awertendo il personale di stare in guardia.

Appendice
Sicurezza in breve

Le seguenti liste e grafici vi forniscono una versione di rapida consultazione dei metodi dell'ingegneria sociale discussi nei capitoli dal 2 al 14 e delle procedure di verifica spiegate nel *Vademecum.* Potete adattare questi consigli alla vostra organizzazione e metterli a disposizione del personale nel momento in cui sorgono problemi relativi alla sicurezza delle informazioni.

IDENTIFICARE UN ATTACCO ALLA SICUREZZA

Queste tabelle e checklist vi aiuteranno ad accorgervi di un attacco in corso.

Il ciclo dell'ingegneria sociale

Azione	*Descrizione*
Ricerche	Possono comprendere le informazioni pubbliche come le relazioni annuali e alla commissione di Borsa, gli opuscoli di marketing, le richieste di brevetto, gli articoli usciti sui giornali e sulle riviste del settore, i contenuti del sito web, e anche la pesca nei cassonetti.
Sviluppo di un rapporto di fiducia	Uso di informazioni interne, fingersi un'altra persona, citare persone note alla vittima, richiesta di aiuto o presentarsi come dirigente.
Sfruttamento della fiducia	Domandare informazioni o azioni da parte della vittima. Nella stangata inversa, convincere la vittima a chiedere aiuto all'attaccante.

Utilizzo delle informazioni	Se l'informazione ottenuta è solo un passo verso la meta finale, l'attaccante ritorna all'inizio del ciclo fino a quando non ha ottenuto quel che cerca.

Classici metodi dell'ingegneria sociale

- Fingersi un collega.
- Fingersi dipendente di un fornitore, di una consociata oppure un tutore dell'ordine.
- Fingersi persona dotata di autorità.
- Fingersi un nuovo assunto che chiede una mano.
- Fingersi un fornitore o un fabbricante di sistemi che telefona per offrire un aggiornamento o un patch al sistema.
- Offrire aiuto in caso di problemi, poi fare in modo che il problema si presenti realmente, convincendo così la vittima a chiedere aiuto.
- Inviare programmi o patch gratis che la vittima deve installare.
- Inviare un virus o un cavallo di Troia come allegato di posta elettronica.
- Usare una falsa finestra pop-up per chiedere all'utente di connettersi di nuovo o registrarsi con una password.
- Catturare le digitazioni della vittima con un sistema o un programma sacrificabile.
- Lasciare un floppy o un CD contenente un software ostile in giro per l'ufficio.
- Usare il gergo e la terminologia di chi è addentro per guadagnarsi la fiducia.
- Offrire un premio a chi si registra a un sito web con username e password.
- Lasciare un documento o un file nella sala posta aziendale per consegna interna.
- Modificare l'intestazione del fax affinché sembri provenire dall'interno.
- Chiedere al banco accoglienza di ricevere e inoltrare un fax.
- Chiedere il trasferimento di un file in altra localizzazione che sembri interna all'azienda.
- Ottenere e impostare una casella vocale perché una eventuale telefonata di controllo faccia sembrare l'attaccante persona appartenente all'azienda.
- Fingere di essere di un'altra sede dell'azienda e chiedere l'accesso in loco alla posta elettronica.

Segni premonitori di attacco

- Rifiuto di dare un numero cui richiamare.
- Richieste fuori dall'ordinario.
- Pretese di posizione dirigenziale.
- Urgenza.
- Minacce di conseguenze spiacevoli in caso di non obbedienza.
- Segni di nervosismo quando interrogato.
- Citazione di nomi importanti.
- Lusinghe o piaggeria.
- Corteggiamento.

Classici bersagli degli attacchi

Tipo di bersaglio	*Esempi*
Ignari del valore delle informazioni	Addetti all'accoglienza, centralinisti, segretari, custodi
Privilegi speciali	Assistenza tecnica generica o informatica, amministratori di sistema, operatori ai computer, amministratori del sistema telefonico
Fabbricante/ fornitore	Produttori di hardware e software e di sistemi di caselle vocali e segreterie telefoniche
Settori specifici	Contabilità, risorse umane

Fattori che rendono le aziende più vulnerabili agli attacchi

- Grande numero di dipendenti.
- Più sedi e stabilimenti.
- Informazioni sulla reperibilità dei dipendenti lasciate nei messaggi delle caselle vocali.
- Informazioni sui telefoni interni accessibili.
- Carenza di training alla sicurezza.
- Assenza di un sistema di classificazione dei dati.
- Assenza di un piano di segnalazione incidenti/risposta.

VERIFICA E CLASSIFICAZIONE DEI DATI

Queste tabelle e grafici vi aiuteranno a reagire alle richieste di informazioni o azioni che potrebbero essere in realtà attacchi di ingegneri sociali.

Procedure per la verifica dell'identità

Azione	*Descrizione*
Identificazione di chiamata	Verificate che la chiamata sia interna e che il nome o il numero di interno corrisponda all'identità di chi telefona.
Richiamare	Cercate nell'elenco aziendale la persona che vi ha fatto la richiesta e richiamatela all'interno che vi compare.
Garanzia	Domandate a un dipendente fidato di garantire l'identità del richiedente.
Segreto condiviso	Richiedete un segreto condiviso aziendale come un codice giornaliero o una password.
Superiore o capufficio	Contattate immediatamente un superiore del richiedente per domandare una verifica dell'identità e della carica ricoperta.
E-mail sicura	Esigete un messaggio con firma digitale.
Riconoscimento diretto della voce	Quando si tratta di persona nota al dipendente, verificare la voce.
Password dinamiche	Verificate con una password dinamica come una Secure ID o un altro strumento di autentica sicura.
In carne e ossa	Domandate al richiedente di presentarsi di persona con tesserino o altro documento d'identità.

Procedure di verifica dello status del dipendente

Azione	*Descrizione*
Controllo elenco dipendenti	Verificate che il richiedente compaia nell'elenco online.
Verifica presso il capoufficio del richiedente	Telefonate al suo superiore usando il numero che compare in elenco.
Verifica nell'ufficio o settore del richiedente	Telefonate al suo ufficio o settore per sentire se è ancora nei ranghi aziendali.

Procedure per verificare il diritto alle informazioni

Azione	*Descrizione*
Consultare l'elenco incarichi/uffici/ responsabilità	Controllare gli elenchi dei dipendenti che hanno accesso a specifiche informazioni riservate.
Ottenere l'autorizzazione dal capoufficio	Contattate il vostro capoufficio o quello del richiedente per essere autorizzati a esaudire la richiesta.
Ottenere l'autorizzazione dal detentore informazioni o dal suo delegato	Domandate al detentore informazioni se il richiedente ha diritto d'accesso.
Ottenere l'autorizzazione tramite strumento automatizzato	Verificate il personale autorizzato nel database proprietario.

Criteri per verificare i non dipendenti

Criteri	*Azione*
Rapporto	Verificate che la ditta del richiedente abbia un rapporto come fornitore, partner strategico o altro adatto.
Identità	Verificate l'identità e incarico del richiedente presso la ditta fornitrice/consociata.
Accordo di riservatezza	Verificate che il richiedente abbia firmato un accordo che lo vincola al riserbo.
Accesso	Segnalate la richiesta alla direzione quando le informazioni sono classificate dal livello Uso interno in su.

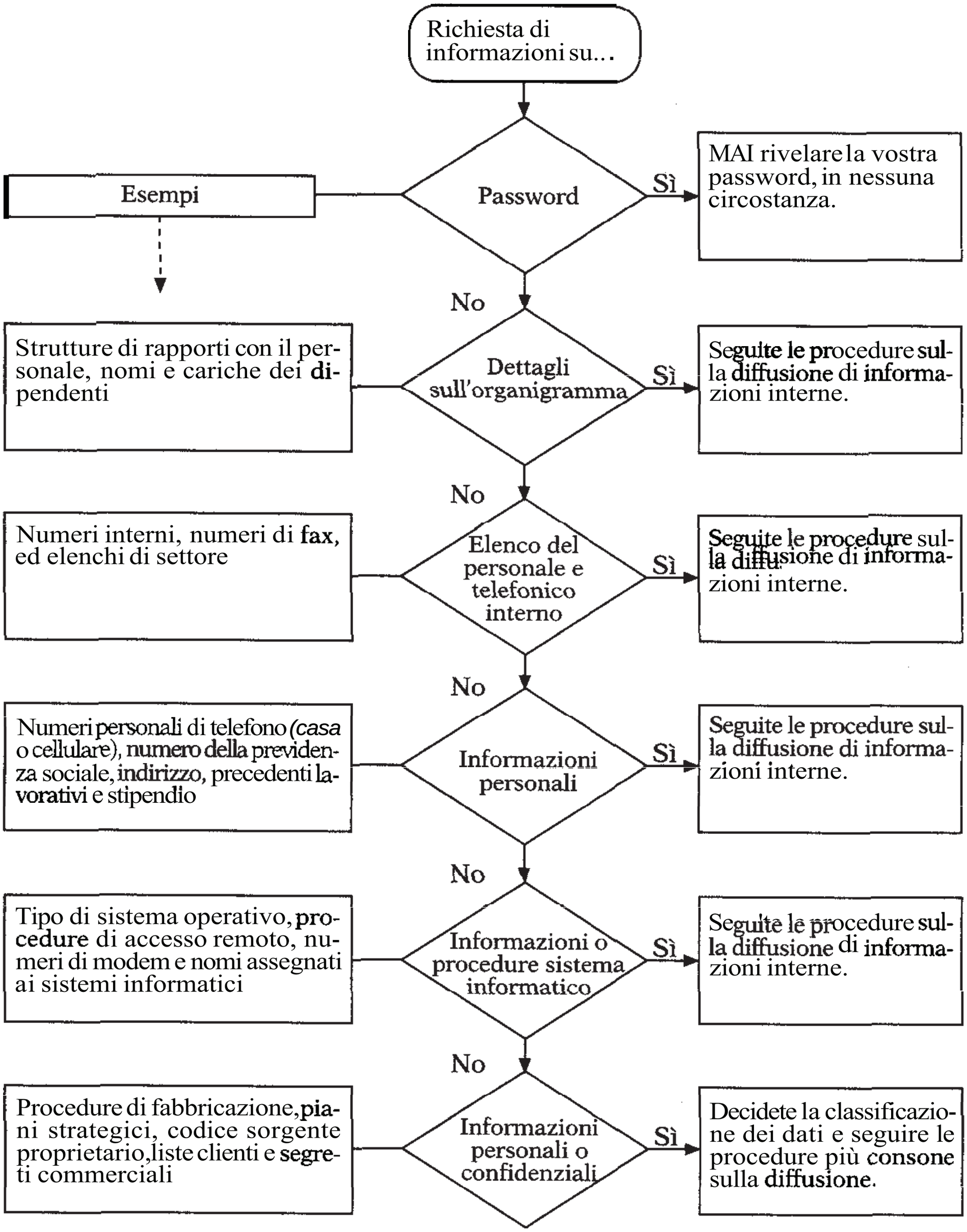
Classificazione dei dati

Classificazione	*Descrizione*	*Procedura*
Pubblici	Possono essere diffusi liberamente al pubblico.	Nessuna verifica.

Classificazione	*Descrizione*	*Procedura*
Interni	Per uso interno all'azienda.	Verificate l'identità del richiedente come dipendente attivo o l'accordo di riservatezza e l'approvazione della dirigenza nel caso di non dipendenti.
Personali	Informazioni di natura personale intese per esclusivo utilizzo interno all'azienda.	Verificate l'identità del richiedente come dipendente attivo o non dipendente autorizzato. Controllate presso le risorse umane la possibilità di svelare informazioni personali a dipendenti o richiedenti esterni autorizzati.
Confidenziali	Da condividere solo con persone con accesso indiscusso alle informazioni entro l'azienda.	Verificate l'identità del richiedente e la sua autorizzazione alle informazioni presso il detentore informazioni designato, e date le informazioni solo dopo assenso scritto del direttore *o* del detentore informazioni o del suo delegato. Controllate l'accordo di riservatezza conservato in archivio. Soltanto il personale della direzione può dare questo tipo di informazioni a chi non è dipendente dell'azienda.

Le domande auree

Come faccio a sapere che questa persona è effettivamente chi sostiene di essere? Come faccio a sapere che questa persona è autorizzata ad avanzare una simile richiesta?

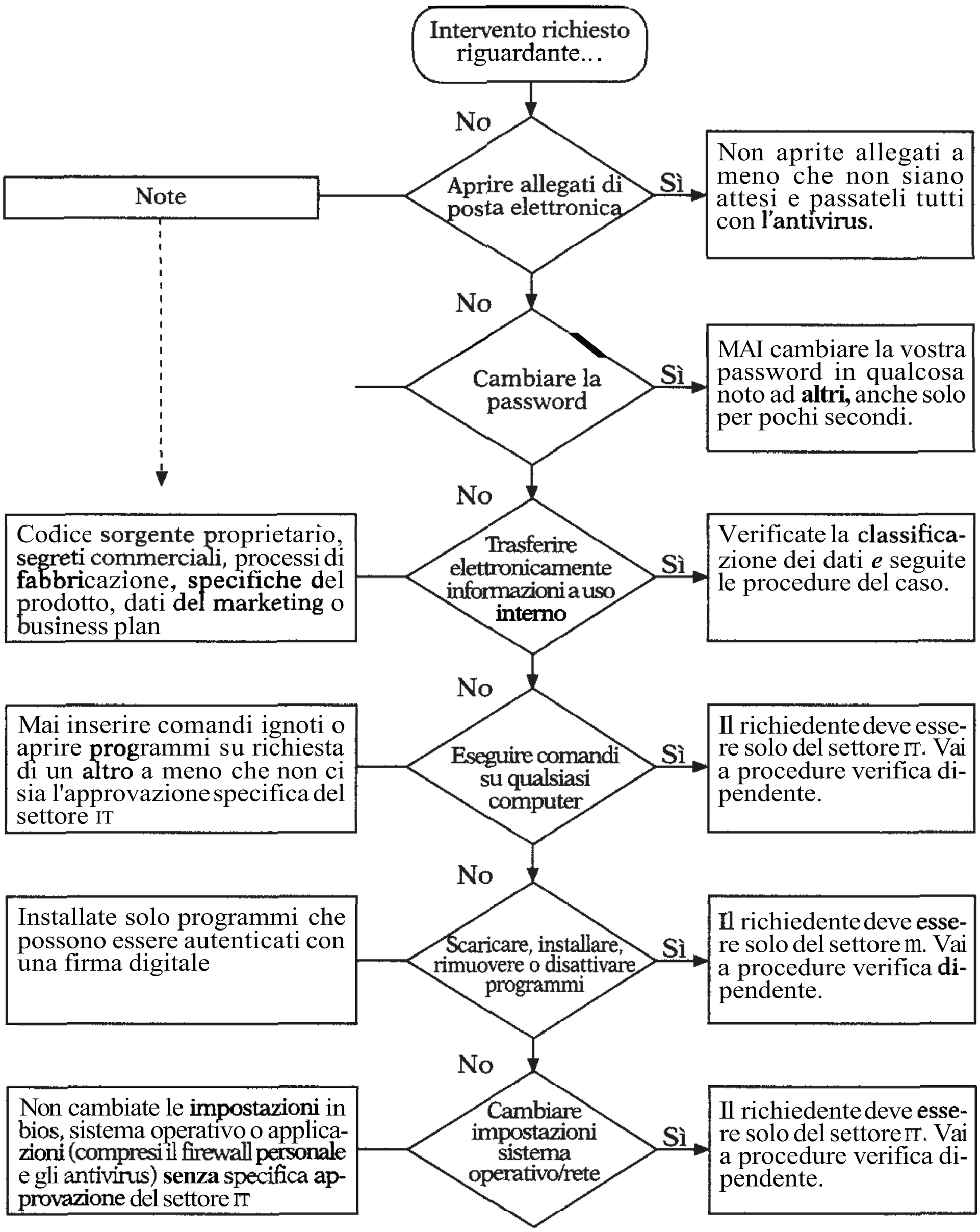

Richiesta di informazioni su...
Password
Sì
MAI rivelare la vostra password, in nessuna circostanza.
Esempi
No
Dettagli sull'organigramma
Sì
Strutture di rapporti con il personale, nomi e cariche dei dipendenti
Seguite le procedure sulla diffusione di informazioni interne.
No
Elenco del personale e telefonico interno
Sì
Numeri interni, numeri di fax, ed elenchi di settore
Seguite le procedure sulla diffusione di informazioni interne.
No
Informazioni personali
Sì
Numeri personali di telefono (casa o cellulare), numero della previdenza sociale, indirizzo, precedenti lavorativi e stipendio
Seguite le procedure sulla diffusione di informazioni interne.
No
Informazioni o procedure sistema informatico
Sì
Tipo di sistema operativo, procedure di accesso remoto, numeri di modem e nomi assegnati ai sistemi informatici
Seguite le procedure sulla diffusione di informazioni interne.
No
Informazioni personali o confidenziali
Sì
Procedure di fabbricazione, piani strategici, codice sorgente proprietario, liste clienti e segreti commerciali
Decidete la classificazione dei dati e seguire le procedure più consone sulla diffusione.

Tutte le informazioni devono essere considerate sensibili a meno che non siano designate per la diffusione al pubblico.

Rispondere a una richiesta di intervento

Le regole auree

Mai fidarsi automaticamente di nessuno senza previa verifica.
Bisogna incoraggiare il personale a contestare le richieste.


Intervento richiesto riguardante...
Note
No
Aprire allegati di posta elettronica
Sì
Non aprite allegati a meno che non siano attesi e passateli tutti con l'antivirus.
No
Cambiare la password
Sì
MAI cambiare la vostra password in qualcosa noto ad altri, anche solo per pochi secondi.
No
Codice sorgente proprietario, segreti commerciali, processi di fabbricazione, specifiche del prodotto, dati del marketing o business plan
Trasferire elettronicamente informazioni a uso interno
Sì
Verificate la classificazione dei dati e seguite le procedure del caso.
No
Mai inserire comandi ignoti o aprire programmi su richiesta di un altro a meno che non ci sia l'approvazione specifica del settore IT
Eseguire comandi su qualsiasi computer
Sì
Il richiedente deve essere solo del settore IT. Vai a procedure verifica dipendente.
No
Installate solo programmi che possono essere autenticati con una firma digitale
Scaricare, installare, rimuovere o disattivare programmi
Sì
Il richiedente deve essere solo del settore IT. Vai a procedure verifica dipendente.
No
Non cambiate le impostazioni in bios, sistema operativo o applicazioni (compresi il firewall personale e gli antivirus) senza specifica approvazione del settore IT
Cambiare impostazioni sistema operativo/rete
Sì
Il richiedente deve essere solo del settore IT. Vai a procedure verifica dipendente.

Tutti gli interventi che fate per conto terzi possono compromettere i beni della vostra azienda. Verificate. Verificate. Verificate.

Fonti

Capitolo 1

Buck Bloombecker, *Spectacular Computer Crimes: What They Are and How They Cost American Business Half a Billion Dollars a Year*, Irwin Professional Publishing, 1990.

Jonathan Littman, *The Fugitive Game: Online with Kevin Mitnick*, Little Brown & Co., Chicago 1997.

Adam L. Penenberg, *The Demonizing of a Hacker*, "Forbes", 19 aprile 1999.

Capitolo 2

La storia di Stanley Rifkin è ricostruita in base a questi resoconti:

Computer Security Institute, *Financial Losses Due to Internet Intrusion, Trade Secret Theft and Other Cyber Crimes Soar*, comunicato stampa (s.i.d.).

Edward Jay Epstein, *The Diamond Znvention*, inedito.

Rev. David Holwick, resoconto inedito.

Lo stesso Rifkin è stato tanto gentile da segnalare che le varie versioni della sua impresa differiscono dal momento che ha protetto il suo anonimato rifiutando le interviste.

Vademecum

Robert B. Cialdini, *Influence: Science and Practice*, quarta edizione, Allyn and Bacon, 2000.

Robert B. Cialdini, *The Science of Persuasion*, "Scientific American", 284:2, febbraio 2001.

Appendice

Alcune politiche presentate in questo capitolo si basano su alcune idee contenute in Charles Cresson Wood, *Information Security Policies Made Easy*, Baseline Software, 1999.

Ringraziamenti

Da Kevin Mitnick

La vera amicizia è stata definita come una sola mente in due corpi. Sono poche le persone nella vita di chiunque che possono essere definite veri amici. Jack Biello era una persona amabile e premurosa scagliatasi contro le straordinarie angherie che ho subito per colpa di giornalisti poco etici e di burocrati zelanti. È stato il portavoce del movimento Free Kevin e uno straordinario autore di articoli incalzanti contenenti le informazioni che il governo non voleva farvi conoscere. Jack era sempre pronto a parlare senza paura in mia difesa e a preparare insieme a me articoli e discorsi, diventando a un certo punto il mio "ufficiale di collegamento" con i media.

Perciò questo libro è dedicato con amore al mio più caro amico Jack Biello, la cui recente morte dovuta a un tumore, proprio mentre finivamo il manoscritto, mi ha lasciato un'enorme sensazione di tristezza e vuoto.

Questo libro non sarebbe stato possibile senza l'amore e l'appoggio della mia famiglia. Mia madre, Shelly Jaffe, e la nonna Reba Vartanian mi hanno regalato amore e appoggio incondizionato da quando sono nato. Sono stato fortunato a crescere con una madre tanto dolce e premurosa, che considero la mia migliore amica. La nonna è stata per me come una seconda mamma, mi ha dato tutte le attenzioni e l'affetto che solo una madre può regalare. Queste persone premurose e compassionevoli mi hanno insegnato a pensare agli altri e a dare sempre una mano ai meno fortunati. Imitando questo loro dare e amare, in un certo senso sto seguendo la loro traiettoria esistenziale. Spero mi perdoneranno se le ho trascurate mentre scrivevo il libro, dimenticando di andarle a trovare a causa del lavoro e delle sca-

denze. Questo libro non sarebbe stato possibile senza il loro amore e appoggio incessante che non potrò mai dimenticare.

Quanto vorrei che papà, Alan Mitnick, e mio fratello Adam fossero vissuti abbastanza da stappare una bottiglia di champagne assieme a me nel giorno dell'uscita del libro. Mio padre, rappresentante di commercio e imprenditore, mi ha insegnato tante cose utili che non scorderò mai. Ho avuto la fortuna di stargli accanto durante il suo ultimo mese di vita per dargli tutto il conforto che potevo, anche se è stata un'esperienza lancinante da cui non mi sono ancora ripreso.

Mia zia Chickie Leventhal avrà sempre un posto speciale nel mio cuore. Anche se è rimasta scossa da alcuni stupidi errori che ho commesso, è sempre stata disponibile con il suo amore e le sue attenzioni. Nel periodo in cui mi sono dedicato in *toto* a questo libro, ho sacrificato tante occasioni per unirmi a lei, a mio cugino Mitch Leventhal e al fidanzato della zia, il dottor Robert Berkowitz, nella celebrazione settimanale del Sabbath.

Devo anche rivolgere i miei più sentiti ringraziamenti al fidanzato di mia madre, Steven Knittle, sempre pronto a darmi il cambio quando bisognava dare amore e sostegno alla mamma.

Anche il fratello di papà merita un encomio. Potrei dire che ho ereditato il bernoccolo dell'ingegnere sociale da zio Mitchell, che sapeva manovrare il mondo e la gente in modi che non credo potrò mai capire, men che meno dominare. Per sua fortuna non ha mai avuto la mia passione per i computer negli anni in cui ha sfruttato il suo fascino per raggirare chi voleva. Il titolo di grande maestro dell'ingegneria sociale sarà sempre suo.

Scrivendo queste note di ringraziamento capisco che ci sono tante persone da citare per l'amore, l'amicizia, l'aiuto che mi hanno dato. Non riesco nemmeno a ricordare i nomi di tutta la gente gentile e generosa incontrata in questi ultimi anni, ma basti dire che ci vorrebbe un computer per archiviarli tutti. Tante persone di tutto il mondo mi hanno inviato parole di incoraggiamento e lode, e le loro lettere hanno significato molto per me, soprattutto quando ne avevo un gran bisogno.

Sono soprattutto grato ai sostenitori che mi sono rimasti accanto sprecando tempo ed energie preziose per far arrivare il verbo a chiunque fosse disposto ad ascoltare, esprimendo le loro obiezioni all'ingiusto trattamento da me subito e alle esagerazioni create da quanti cercavano di approfittarsi del "mito di Kevin Mitnick".

Ho avuto la fortuna incredibile di fare coppia con il noto scrittore Bill Simon, con cui sono riuscito a produrre proficuamente nonostante le diverse modalità lavorative. Bill è superorganizzato, si alza presto e lavora lento e metodico. Gli sono molto grato per essere stato tanto gentile da accettare i miei tempi da anima-

le notturno. Il mio impegno in questo progetto e le interminabili giornate di lavoro mi tenevano sveglio fino all'alba, andando a scontrarmi contro la programmazione regolare di Bill.

Non solo ho avuto la fortuna di fare squadra con una persona capace di trasformare le mie idee in frasi degne di un lettore sofisticato, ma devo aggiungere che Bill è anche (quasi sempre) un uomo molto paziente che si è adattato al mio stile di attenzione ai dettagli tipico del programmatore. E ce l'abbiamo fatta. Però vorrei scusarmi con lui in questi ringraziamenti garantendogli che rimpiangerò sempre di averlo costretto per colpa della mia tendenza alla pignoleria sui dettagli a farsi trovare in ritardo con una scadenza, per la prima e unica volta nella sua lunga carriera di autore. Bill ha un orgoglio professionale che finalmente ho compreso, e spero di fare altri libri insieme.

Uno dei momenti luminosi di questa impresa autoriale è stata la mia permanenza a casa Simon a Rancho Santa Fe a farmi coccolare durante il lavoro dalla moglie di Bill, Arynne. La sua conversazione e la sua cucina battagliano nei miei ricordi per il diritto alla medaglia d'oro dei ringraziamenti. Arynne è una donna preziosa e saggia, piena di allegria, che ha creato una casa di grande bellezza e calore. E non berrò mai più una bevanda dietetica senza risentire la sua voce che mi ammonisce sui pericoli dell'aspartame.

Stacey Kirkland significa molto per me. Ha impegnato molte ore del suo tempo per assistermi al Macintosh a preparare tabelle e grafici che avrebbero aggiunto una dimensione visiva alle mie idee. L'ammiro molto, è una persona davvero dolce e attenta che si merita le cose più belle dalla vita. Mi ha incoraggiato da amica che teneva molto al mio benessere, ed è una persona cui tengo molto anch'io. Vorrei ringraziarla per tutto il suo aiuto e per essermi stata accanto nei momenti di necessità.

Alex Kasper, di Nexspace, non è solo il mio migliore amico ma anche un socio e un collega. Assieme abbiamo condotto un talk show radiofonico, *Il lato oscuro di Internet*, su KFI AM 640 di Los Angeles sotto la mano abile del direttore della programmazione David G. Hall. Alex ha gentilmente fornito i suoi inestimabili consigli per questo progetto editoriale. La sua influenza è sempre stata positiva, con una gentilezza e generosità che spesso si espandeva ben oltre la mezzanotte. Di recente, assieme ad Alex, ho prodotto un video per aiutare le imprese a formare il personale alla prevenzione degli attacchi degli ingegneri sociali.

Paul Dryrnan, di Informed Decision, è più di un amico di famiglia. Questo investigatore privato rispettato e affidabile mi ha aiutato a capire le tendenze e le procedure delle indagini di base. La sua esperienza ed erudizione mi hanno aiutato ad affrontare i problemi della sicurezza del personale descritti nella quarta parte di questo libro.

Una delle mie migliori amiche, Candi Layman, non mi ha fatto mai mancare amore e appoggio. È una persona veramente meravigliosa meritevole di stima. Durante gli anni tragici del mio passato mi ha sempre dato la sua amicizia e i suoi incoraggiamenti. Sono molto fortunato a conoscere un essere umano tanto meraviglioso e premuroso, e vorrei ringraziarla per essermi stata accanto.

È garantito che il mio primo assegno delle royalty servirà a pagare le bollette del cellulare per tutte le ore passate a discutere con Erin Finn, senza alcun dubbio una mia anima gemella. Siamo tanto simili da fare paura. Tutti e due adoriamo la tecnologia, e abbiamo gli stessi gusti quanto a cibi, musica e film. La AT&T Wireless sta andando in bancarotta per avermi dato "notte e fine settimana gratis" per le chiamate a casa sua a Chicago. Perlomeno non uso più il piano Kevin Mitnick. Il suo entusiasmo e la sua fede in questo libro mi hanno dato coraggio. Sono dawero fortunato ad avere un'amica del genere.

Non vedo l'ora di ringraziare le persone coinvolte nella mia carriera professionale e che sono tanto dedite. Le mie conferenze sono gestite da Amy Gray (una persona onesta e attenta che ammiro e adoro). David Fugate della Waterside Productions è un agente letterario che mi ha sostituito in tante occasioni prima e dopo la firma del contratto. E sono sicuro che l'avvocato Gregory Vinson di Los Angeles, della mia squadra di difensori nella battaglia lunga un anno con il governo, potrebbe essere associato al ringraziamento per la pazienza di Bill messa a dura prova dalla mia mania dei dettagli. Ha vissuto la medesima esperienza con me quando mi scriveva gli esposti.

Ho avuto tanti trascorsi con gli avvocati che sono smanioso di esprimere la mia gratitudine ai legali che durante gli anni di rapporti negativi con la magistratura si sono offerti di aiutami quando ne avevo una necessità disperata. Dalle parole gentili fino al coinvolgimento totale nel mio caso, ne ho conosciuti tanti che stonano con lo stereotipo dell'azzeccagarbugli egoista. Sono giunto a rispettare, ammirare e apprezzare le gentilezza e la generosità che tanti mi hanno offerto senza limiti. Tutti si meriterebbero di essere ringraziati con un intero paragrafo di elogi. Perlomeno li citerò per nome, perché ognuno di loro vive nel mio cuore avvolto nella gratitudine: Greg Aclin, Bob Carmen, John Dusenbury, Sherman Ellison, Omar Figueroa, Carolyn Hagin, Rob Hale, Alvin Michaelson, Ralph Peretz, Vicki Podberesky, Donald C. Randolph, Dave Roberts, Alan Rubin, Steven Sadowski, Tony Serra, Richard Sheman, Skip Slates, Karen Smith, Richard Steingard, l'onorevole Robert Talcott, Barry Tarlo ~John Yzurdiaga e Gregory Vinson.

Sono estremamente grato per l'occasione che la John Wiley &

Sons mi ha regalato con questo libro e per la loro fiducia in un autore esordiente. Vorrei ringraziare i seguenti dipendenti della Wiley che hanno reso possibile questo sogno: Ellen Gerstein, Bob Ipsen, Carol Long (mia editor e stilista) e Nancy Stevenson.

Altri familiari, amici e collaboratori che mi hanno dato consigli e appoggio, e si sono offerti in tanti modi, meritano di essere ricordati e ringraziati. Sono: J.J. Abrams, David Agger, Bob Arkow, Stephen Barnes, dottor Robert Berkowitz, Dale Coddington, Eric Corley, Delin Conneny, Ed Cummings, Art Davis, Michelle Delio, Sam Downing, John Draper, Paul Dryman, Nick Duva, Roy Eskapa, Alex Fielding, Lisa Flores, Brock Frank, Steve Gibson, Jerry Greenblatt, Greg Grunberg, Bill Handle, David *G.* Hall, Dave Harrison, Leslie Herman, Jim Hill, Dan Howard, Steve Hunt, Rez Johar, Steve Knittle, Gary Kremen, Barry Krugel, Adrian Lamo, Leo Laporte, Mitch Leventhal, Cynthia Levin, CJ Little, Jonathan Littman, Mark Maifrett, Brian Martin, Forrest McDonald, Kerry McElwee, Alan McSwain, Elliott Moore, Michael Morris, Eddie Munoz, Patrick Norton, Shawn Nunley, Brenda Parker, Chris Pelton, Kevin Poulsen, Scott Press, Linda e Art Pryor, Jennifer Reade, Israel e Rachel Rosencrantz, Mark Ross, William Royer, Irv Rubin, Ryan Russell, Neil Saavedra, Wynn Schwartu, Pete Shipley, Joh Siff, Dan Sokol, Trudy Spector, Matt Spergel, Eliza Amadea Sultan, Douglas Thomas, Roy Tucker, Bryan Turbow, Ron Wetzel, Don David Wilson, Darci Wood, Kevin Wortman, Steve Wozniak e tutti i miei amici sul ripetitore W6NUT (147,435 Mhz) di Los Angeles.

E anche il mio responsabile della libertà vigilata Larry Hawley si merita uno speciale ringraziamento, per avermi dato il permesso di fungere da consigliere e consulente su temi relativi alla sicurezza scrivendo questo libro.

Per finire devo ringraziare i tutori dell'ordine. Non ho nulla contro queste persone che fanno solo il loro dovere. Credo sul serio che mettere l'interesse di tutti davanti al proprio e dedicare la vita al servizio del pubblico sia una scelta da rispettare, e anche se ogni tanto sembro arrogante voglio che sappiate che amo il mio paese e farei tutto il possibile per farne il posto più sicuro al mondo, che è esattamente una delle ragioni per cui ho scritto questo libro.

Da *Bill Simon*

Sono convinto che là fuori ci sia la persona ***giusta*** per ognuno di noi, solo che qualcuno non è tanto fortunato da trovarla. Altri lo sono. Io sono stato tanto fortunato da aver già vissuto tanti anni felici (e prevedo di passarne tanti altri) con una delle mera-

viglie del creato, mia moglie Arynne. Se mai dimentico la fortuna che mi è toccata, mi basta ascoltare tutti coloro che cercano e adorano la sua compagnia. Arynne, ti ringrazio perché vivi la tua vita con me.

Mentre scrivevo questo libro ho contato sull'aiuto di un gruppo di amici leali che hanno garantito che Kevin e io riuscissimo a combinare fatti e fantasia in questo libro insolito. Ognuno di loro è un valore vero e leale e sa che sarà interpellato per il mio prossimo progetto editoriale. In ordine alfabetico: Jean-Claude Beneventi, Linda Brown, Walt Brown, generale Don Johnson, Dorothy Ryan, Guri Stark, Chris Steep, Michael Steep e John Votaw.

Un riconoscimento speciale va a John Lucich, presidente del Network Security Group, disposto a dedicare tempo a un amico, e a Gordon Garb, che si è prestato gentilmente a qualche telefonata sulle attività IT.

Certe volte nella vita un amico si guadagna un posto speciale presentandoti qualcun altro che diventa un amico intimo. All'agenzia letteraria Waterside Production di Cardiff, in California, l'agente David Fugate ha concepito l'idea di questo libro e mi ha associato al futuro amico Kevin. Grazie, David. E a capo della Waterside c'è l'impareggiabile Bill Gladstone, che riesce a tenermi impegnato in un progetto di libro via l'altro: sono felice di averti al mio angolo.

Nella nostra casa-ufficio Arynne è coadiuvata da uno staff capace che comprende la segretaria Jessica Dudgeon e la governante Josie Rodriguez.

Ringrazio i miei genitori Marjorie e J.B. Simon, che vorrei fossero ancora qui per godersi il mio successo come autore. Ringrazio anche mia figlia Victoria. Ogni volta che sono con lei capisco quanto l'ammiro, quanto la rispetto, quanto ne sia orgoglioso.

Indice

Pag. 11 Premessa di Steve Wozniak

13 Prefazione

19 Introduzione

Prima parte

21 Dietro le quinte

23 1. L'anello più debole della sicurezza

Seconda parte

33 L'arte dell'attaccante

35 2. Quando un'informazione innocua non lo è

48 3. L'attacco diretto: basta chiedere

56 4. Costruire la fiducia

68 5. "Posso aiutarla?"

86 6. "Può aiutarmi?"

100 7. Siti civetta e allegati pericolosi

111 8. Sfruttare simpatia, senso di colpa e intimidazione

135 9. La stangata inversa

Terza parte
149 Allarme intruso

151 10. Entrare nella struttura
173 11. Fondere tecnologia e ingegneria sociale
193 12. Attacchi al livello più basso
207 13. Attacchi più elaborati
222 14. Spionaggio industriale

Quarta parte
239 Innalzare la sbarra

241 15. Presa di coscienza e training sulla sicurezza delle informazioni

255 Vademecum per la sicurezza delle informazioni aziendali

309 Appendice
Sicurezza in breve

317 Fonti

319 Ringraziamenti